军事网络技术基础

代科学　孙合敏　黄志良　等著

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书以军事信息系统网络为主要背景，介绍与之相关的计算机网络基本知识和基础技术。本书内容主要包括军事网络基本概念、计算机网络基本原理、数据通信基础技术、局域网和广域网典型技术与设备，以及军事网络服务、网络管理、网络安全等方面的知识和技术。

本书在介绍计算机网络基础原理与技术的同时，突出网络技术在军事信息系统中的适用性，可作为军事网络应用领域或相关专业培训的教材或参考书。

图书在版编目（CIP）数据

军事网络技术基础/代科学等著. —北京：电子工业出版社，2017.11

ISBN 978-7-121-32960-9

Ⅰ. ①军… Ⅱ. ①代… Ⅲ. ①计算机网络－应用－军事技术－基本知识 Ⅳ. ①E919

中国版本图书馆 CIP 数据核字（2017）第 262437 号

策划编辑：李 洁（lijie@phei.com.cn）
责任编辑：张 京
印 刷：
装 订：
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×1092 1/16 印张：12.5 字数：320 千字
版 次：2017 年 11 月第 1 版
印 次：2017 年 11 月第 1 次印刷
定 价：49.90 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：lijie@phei.com.cn。

前　言

进入 21 世纪以来，军事信息系统已由局部互连、网络互连向以网络为中心的体系架构发展，实现了更大地域、更广领域的网络化。计算机网络在军事信息获取、传输、处理、管理与应用中具有重要的基础地位，可以说是军事信息系统的“神经”和“血管”。本书从计算机网络技术在军事信息系统中的应用视角出发，遵循“内容与军事结合、为实用服务”的原则，突出相关性、基础性、简要性等特点，专题化介绍军事信息系统中的计算机网络基本理论与基础技术。

本书共分 7 章，内容安排如下。

第 1 章为军事网络基本知识，主要介绍军事网络的功能和作用、逻辑结构、组网形式和传输模式，以及计算机网络的数据交换方式、网络体系结构、TCP/IP 参考模型及其协议工作过程。

第 2 章为军事网络通信基础，主要介绍数据通信有关概念、传输方式、性能指标，各种编码和调制技术，以及频分复用、时分复用、波分复用和码分复用等信道复用技术。

第 3 章为军事局域网络技术，主要介绍以太网技术、VLAN 虚拟局域网技术、网络接入技术，以及同轴电缆、双绞线、光纤等有线传输介质。

第 4 章为军事广域网络技术，主要介绍 IP 连网技术与子网规划方法，网络互连原理与典型路由策略，宽带 IP 网络与 ATM、SDH、DDN 等广域网络技术，VPN 技术与 MPLS 协议，以及路由器的选购、连接与配置等。

第 5 章为军事网络服务，主要介绍信息网络化服务的体系与实现流程，信息单元即插即用的概念与移动 IP 即插即用技术，服务器知识与 Web 技术等。

第 6 章为军事网络管理，主要介绍军事网络管理需求、内容和方法，SNMP 网络管理协议原理和系统组成，网络故障排除的一般方法、常用命令和典型步骤等。

第 7 章为军事网络安全，主要介绍网络安全隐患、安全系统分类、安全设备功能，数据加密、防火墙、入侵检测、非法外联监控等网络安全技术，以及网络病毒防护等。

本书由代科学负责统稿，编写组成员有代科学、孙合敏、黄志良、郭继光、万歆睿、钱琼芬、黄子俊、徐斌、郭乐江等。感谢所在单位领导和同事给予的支持，感谢中国电科有关院所提供的帮助，感谢国防科技大学李国辉教授、空军预警学院熊家军教授和田康生教授提出的修改意见。本书编写中参考了谢希仁教授等的著作及其他网络资料，一并诚挚感谢所有参考文献的拥有者。本书的出版得到中国博士后科学基金（2015M581146）和单位青年基金（2013QNCX0107）资助。

由于编者水平有限，若有错误和疏漏，恳请读者提出宝贵意见和建议。

作　者

2017 年 9 月

目　　录

Chapter 1

第 1 章

军事网络基本知识

【主要内容】 介绍军事网络的基本概念与模型及计算机网络的基本原理，包括军事网络的功能作用、逻辑结构和组网形式，以及计算机网络的数据交换方式、网络体系结构、TCP/IP 参考模型及其协议工作过程。

1.1 军事网络基本概念

广义的军事网络种类非常多，本书主要指基于计算机网络技术构建的军事信息系统网络。计算机网络技术是将多台具有独立功能的计算机互相连接，实现资源共享和信息交换与处理的技术，包括网络体系结构技术、网络协议技术、网络互连技术、网络管理技术、网络安全技术等。计算机网络就是一些互连的、自治的计算机的集合。自 20 世纪 60 年代末诞生计算机网络以来，已被广泛应用于政治、经济、军事、生产及科学技术等各个领域。

军事信息是反映军事活动特征及其发展变化的各种情报、命令、消息、资料的统称。军事信息系统是用于保障军队作战和日常活动的信息系统，主要包括指挥信息系统、作战信息系统和日常业务信息系统等。军事信息系统网络是信息化条件下各层级军事信息系统互连所构成的计算机网络，是军队实施作战指挥、综合保障、部队管理及开展教育训练和日常办公的主要平台。典型的军事信息系统网络有军事指挥系统网络、军事情报系统网络、军事训练系统网络、业务管理系统网络等。

1.1.1 军事网络的功能

军事网络是计算机网络技术的军事应用系统。军事网络在计算机网络软件和协议的管理下，利用网络设备和通信线路，将具有独立功能的多个军事计算机系统（或军事装备/设备）进行互联互通，实现对军事信息的获取、传输、处理、管理和应用，从而为各级指挥机构、部队人员或武器平台等提供军事信息服务。

军事网络的主要功能如下。

1．数据通信

军事网络使分散在不同部门、不同单位，甚至不同地域的军用计算机与计算机之间可以进行通信，互相传送数据，进行信息交换。

2．资源共享

这是军事网络最有吸引力的功能，在网络范围内，用户可以共享软件、硬件、数据等资源，而不必考虑用户及资源的地理位置。

3．协同处理

借助分散在网络中的多台计算机，可以综合处理不同种类、不同粒度、不同时空的军事数据，生产时空统一、要素齐全、理解一致的军事信息，解决单机无法完成的处理任务，达成集中处理才能实现的处理效果。

4．能力整合

网络中的设备与系统可以功能互备、性能均衡。一旦某台计算机出现故障，它的任务可由网络中的其他计算机来完成。当网络中某台计算机负荷过重时，可将新任务分配给网络中较空闲的计算机去完成。

1.1.2 军事网络的作用

军事网络围绕军事决策、军事筹划、军事指挥、军事行动及值班训练、管理保障等军事活动需要，以通信手段为依托，集军事信息收集、组织管理、分析处理、服务应用于一体，为军事人员、武器、系统生成业务信息产品，实现对有关军事信息的网络化共享和联合运用。

军事网络的作用有以下几点。

1．实现军事力量的网络化组织

军事网络可对军事信息生产、管理、使用等各种力量实现网络化管理，对各类信息资源实现网络化组织，增强对军事力量的统管力度，有助于拓展军事信息的运用效益。

2．实现军事数据的网络化处理

军事网络利用网络优势和先进的信息处理技术，对相关军事数据进行多源融合处理、相互补充印证、综合分析挖掘，从而生成更加及时、准确、丰富的军事信息。

3．实现军事信息的网络化服务

军事网络将零散、孤立的军事信息系统连为整体，对各信息用户实现随遇入网、即插即用，按需提供各种粒度的军事信息产品，可大大提高军事信息的利用效率，提高信息服务质量。

4．实现军事系统的网络化管理

军事网络采用网络集群和异地控制等技术，可对有关军事系统进行快速组网、动态管控。通过网络化监控软件可实时监控联网军事系统的信息输入/输出、主要设备和应用软件的状态，及时获得告警提示，及时施行调度控制。

1.1.3　军事网络的能力

军事网络充分发挥多领域、多要素的整体作用，对专业军事信息或综合军事信息实现一体化收集管理、融合处理和服务保障，形成军事网络体系能力。

1．全源信息收集能力

网络化组织各类信息源，可大大提高全域、全维、全谱的信息获取能力。军事网络可以全域收集声、光、电等传感器信息，获取战略、战役、战术级的动向信息、图像信息、目标信息、信号信息等军事信息。

2．高效信息处理能力

军事网络可以对不同来源、用不同手段获取的信息进行融合处理和相互印证，以便生成客观反映、一致理解的军事信息产品，提高信息的时效性、准确性、可靠性。使得信息产品在质量上及时准确、在属性上要素完整、在内容上门类齐全。

3．精准信息服务能力

信息服务是军事网络的出发点和目的，信息服务能力是军事网络最根本的能力。对各类信息产品实行分级分类管控，采取计划推送、专题保障、临机保障、按需定制等方式，可大大缩短信息服务时延，提高信息服务质量。

4．持续信息保障能力

军事网络可为信息资源柔性重组、指挥体系快速重构、武器平台机动部署等应用提供可靠、快速、连续的支撑平台。综合运用全网时间统一、运行状态监控、接替重组等多种手段，可实现军事信息系统冗余配置、异地互备，增强体系化的抗扰抗毁能力。

1.2 军事网络基本模型

1.2.1 军事网络的逻辑结构

军事信息系统网络一般由实现信息获取、信息处理、信息管理和信息应用等独立功能的军事计算机系统组成。这些计算机系统就是网络节点，无论空间分布上的近与远，这些节点按照信息流程、处理规则和保障关系，协调有序地实现网络资源共享。

从逻辑功能上，军事网络的组成节点可划分为信息源节点、信息处理节点、信息管控节点、信息服务节点和信息用户节点等 5 类。物理上它们可能分布各异也可能处于同一节点。

1．信息源节点

信息源节点由各类传感器系统和信息源引接系统组成，按照一定规则向相应的信息处理节点提供原始军事信息，并向信息管控节点上报信息源系统的工作状态信息。

2．信息处理节点

各种信息源提供的信息内容不同，其准确性、精度也不一样，信息处理节点综合运用多种信息融合技术，在不同情况下采用不同的数据处理方式对信息源提供的信息进行处理，使信息要素更全、质量更高，并向信息管控节点上报保障情况，向信息服务节点发送信息产品。

3．信息管控节点

信息管控节点根据军事任务的需要及网络组成节点的状态，完成对军事信息资源的统一调度与管理，完成对军事网络结构的适当调整与控制，以便提高信息保障能力。信息管控节点向信息源节点下达管控指令，向信息处理节点下达信息保障指令，向信息服务节点发送节点管控指令和信息推送指令。

4．信息服务节点

信息服务节点根据军事任务、保障对象的要求和信息的时效性、粒度、用途等特征，向网络中的信息用户提供信息产品。信息服务的目标是做到“四个恰当”，即在恰当的时间、以恰当的形式，将恰当的信息传递到恰当的用户手中。信息服务节点向信息管控节点发送用户需求和信息服务情况，向信息用户节点发送定制或推送的信息产品。

5．信息用户节点

信息用户节点根据军事任务和信息保障关系，通过恰当的方式向相关信息服务节点提出信息需求，从相关信息服务节点获取所需信息产品。

军事网络的逻辑结构关系如图 1-1 所示。

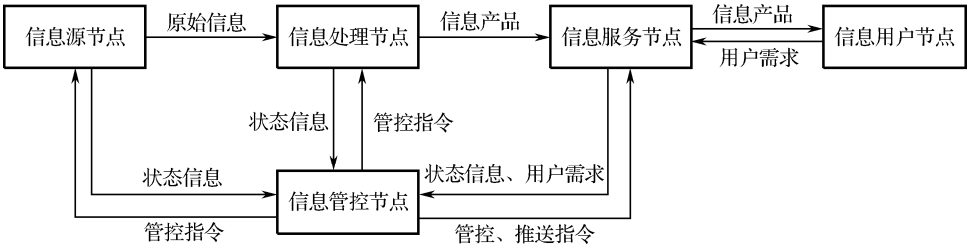


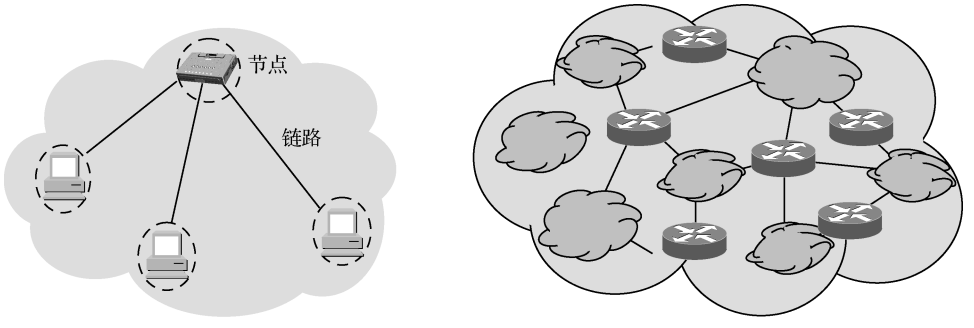
图 1-1　军事网络的逻辑结构关系

军事网络把军事信息收集、处理、分发、管控与应用等信息节点聚合起来，为筹划决策、指挥控制、行动实施等军事活动提供信息保障。其发展趋势是建立军事栅格网，实现信息源“一点入网、全网皆知”，业务信息“分布处理、全网共享”，信息用户“一点接入、按需获取”，以便提高信息的处理与使用效率，缩短军事信息系统的反应时间。

1.2.2　军事网络的组网形式

军事网络是现代通信技术、计算机技术和网络技术在军事系统中应用的产物。从军事信息系统网络的硬件组成看，所涉及的计算机网络设备主要是交换机、路由器、防火墙、集线器、调制解调器等，以及网络服务器、网络工作站和席位计算机等网络工作平台。通信传输介质可以是双绞线、光纤、同轴电缆等有线介质，也可以是红外线、微波、激光等无线介质。

军事网络以“网络为中心”而不以“平台为中心”，通过网络连接各类信息源、信息处理中心和信息用户，实现对各种军事力量、要素、单元的网络化组织运用。从计算机网络的专业角度看，网络是由若干节点（node）和连接这些节点的链路（link）组成的。在组网规模上，军事网络有图 1-2 所示的两种表现形式。其中，图 1-2（a）只由一个网络通信设备将多台独立的军用计算机连接起来，而图 1-2（b）所示的军事网络则是比较常见的网络，它由多个网络设备和多条链路将多个军事网络连接在一起。这里，网络节点是指计算机、交换机、路由器等。



（a）简单的军事网络　　（b）互连的军事网络

图 1-2　军事网络的两种表现形式

实现军事网络互连的设备可分为传输信道、网络交换、信息上报和终端等 4 类设备。网络交换类设备包括网络交换机、多端口服务器和路由器，主要完成地址解析、协议转换、路由选择、链路控制等功能；信息上报类设备指信息报知服务器，主要完成数据收发和处理；终端类设备包括通用数据终端和管理终端，主要完成各种数据业务的人机交互、网络管理及值班管理等工作。大型军事网络的组成如图 1-3 所示。

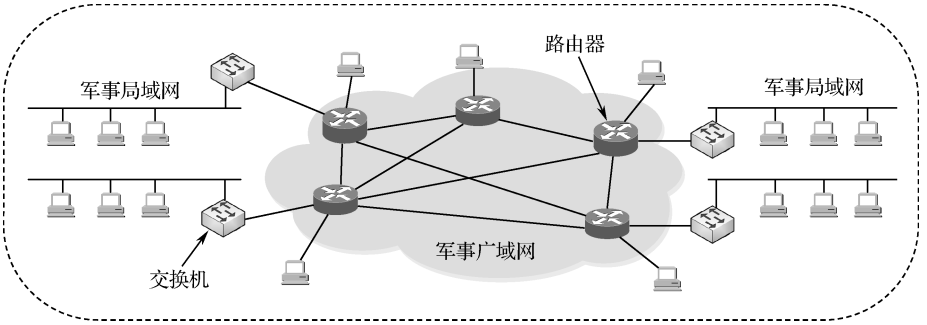


图 1-3　军事网络组成示意图

现代军事网络覆盖范围广、地域分散、空间范围大，可分为军事局域网和军事广域网。典型大型军事信息系统由多个内部局域网络组成，并通过各种网络软/硬件设备互连构成广域网络，将若干个局域网军事信息系统组织成一个更大的网络系统。

1．军事局域网

局域网（Local Area Network，LAN）覆盖的地理范围较小，将一个单位或某个系统有限范围内的本地计算机互连成网。这里，局域网或广域网的概念是按网络的覆盖范围分类的。局域网广泛应用于连接家庭、办公室、校园、指挥所等场所的计算机或工作站，以利于计算机或工作站之间的资源共享和数据通信。

军事信息系统内部的服务器和席位计算机等设备由交换机等网络设备互连，形成一个局域网，然后通过路由器就近接入其他军事网络。大型军事信息系统内部局域网一般采用星形和树形结构相结合的计算机局域网，通过交换机或集线器，利用双绞线或光纤，将有限地理范围内的大量计算机互连一起，实现数据传输和资源共享，如图 1-4 所示。

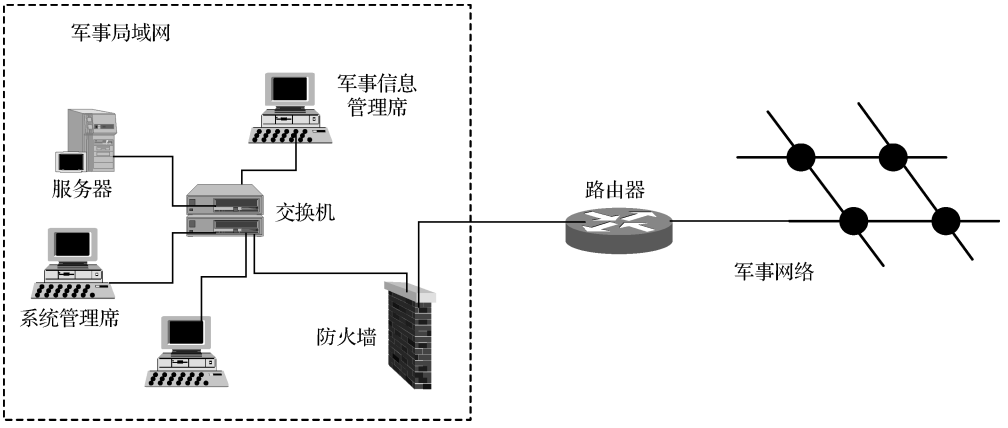


图 1-4　军事局域网与外部网络的连接关系

局域网是计算机网络中非常重要的一个分支，目前最常见的局域网主要是以双绞线、光纤为传输介质的以太网。局域网的特点是结构规则、连接范围小、用户数少、配置容易、数据传输速率高、延迟短、误码率低，可管理性及安全性比较好。

区别于广域网，局域网具有以下特点。

（1）地理分布范较小，一般为数百米至数公里。可覆盖一幢大楼、一所校园或一个企业。

（2）数据传输速率高，一般为 10～100Mbps，已出现速率高达千兆位每秒的局域网。可交换各类数字和非数字（如语音、图像、视频等）信息。

（3）误码率低，一般在 10^{-11}～10^{-8} 以下。这是因为局域网通常采用短距离基带传输，可以使用高质量的传输媒体，从而提高了数据传输质量。

（4）以 PC 为主体，包括终端及各种外设。

（5）协议简单、结构灵活、建网成本低、周期短、便于管理和扩充。

2．军事广域网

广域网（Wide Area Network，WAN）又称远程网，它将地理位置上相距较远的多个局域网或计算机系统，通过通信线路按照网络协议连接起来。网络互连的目的是使一个网络上的用户能访问其他网络上的资源，使不同网络上的用户互相通信和交换信息。要实现网络互连，除了在网络之间至少提供一条物理上连接的链路外，还要通过路由设备采取一些协议规程对这条链路进行控制，才能在不同网络的进程之间实现数据交换。

严格地讲，广域网并不是把计算机用一条传输线路连接起来，而是通过路由器等各种网间互连设备将若干个结构差异大、协议多样、业务多样的局域网组织成一个更大的网络，如图 1-5 所示。

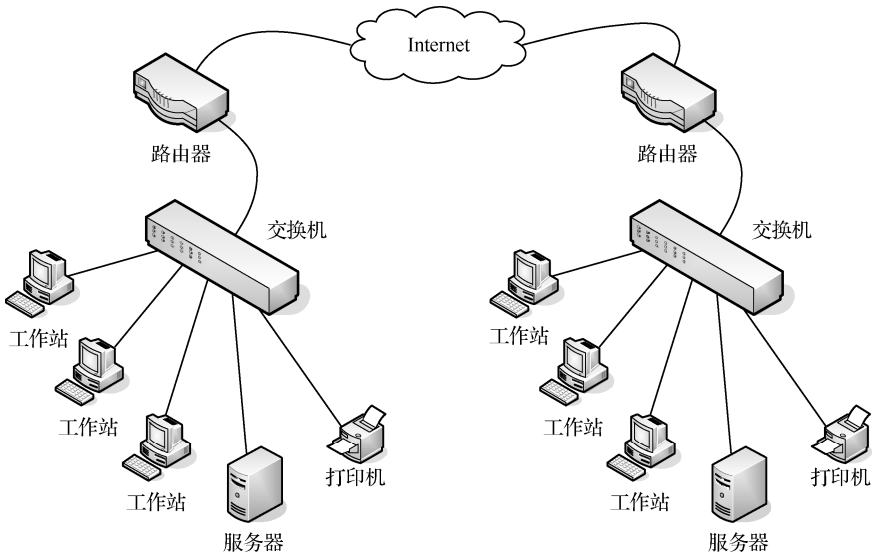


图 1-5　由路由器连接的网络

广域网的覆盖范围从几十公里到几千公里，用于远距离、高速、大容量数据传输。以计算机网络技术构成的军事网络，其中的信息源节点、信息处理节点、信息管控节点、信息服务节点等都通过路由器实现广域互连，从而构成了相关单位的军事信息传输网络，实现军事信息的广域传递与共享，如图 1-6 所示。

军事信息系统网络通常以高速光纤网络为基础，以低速程控电话交换网、短波、卫星、数据链等手段为协助，完成军事信息在各系统之间的传递。军事信息系统一般具备多路由连网能力，使得一个节点可以与多个其他节点相连，确保系统通信畅通，不仅有利于资源共享，也可以从整体上提高网络的可靠性。

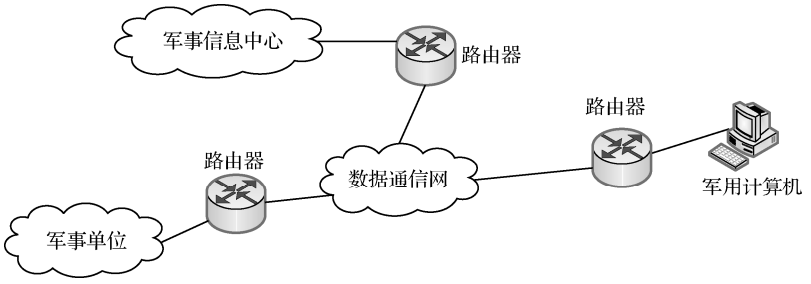


图 1-6　由路由器连接的军事信息传输网络

所以，大型军事信息系统通常采用网状网方式，实现有关军事单位的局域网络互连，如图 1-7 所示。通过路由器将分布在广大地理范围内、不同单位间的各个局域网系统互相连接，构成广域网络，实现军事信息在各个异地甚至异构系统之间的传递。

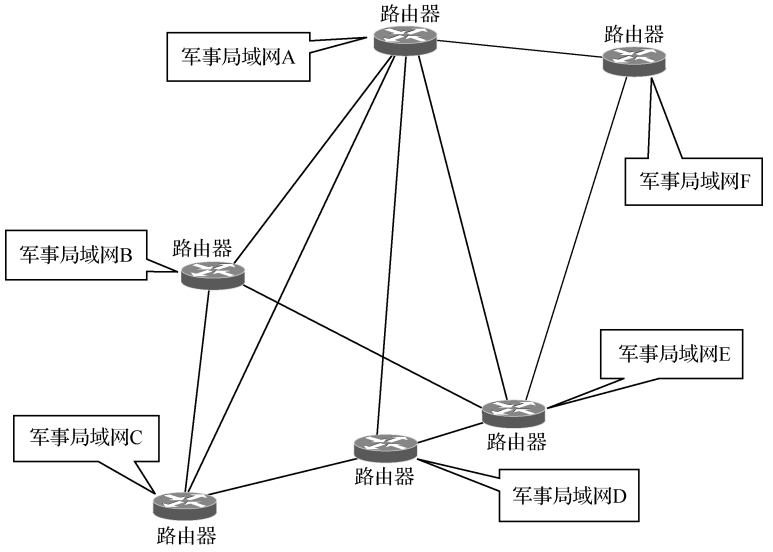


图 1-7　军事广域网络连接示意图

广域网广泛应用于国民经济的许多方面，与局域网既有区别又有联系。随着网络技术特别是以太局域网技术的进步，以及相关设备性价比的提高，构建广域网或局域网所采用的技术正在逐步缩小差别，一些广域网技术和设备也被应用于局域网中，一些以太局域网技术和设备也被用于构建广域网。

1.2.3　军事网络的传输模式

计算机网络中的通信双方是“相互连接”的“自主系统”。“相互连接”的含义是彼此间有可以相互交换信息的信道存在，“自主”是指网络中的通信系统无需外界的支持与控制就能独立运行。这就需要网络双方必须按照约定的规则进行通信，也就是说，计算机系统之间的信息交换必须遵循一定的通信协议。

因此，网络通信双方是通过各自运行网络程序实现信息传输的。无论是网络服务器、网络工作站或席位计算机等网络工作平台，还是交换机、路由器、防火墙等网络互连设备，都要运行一定的网络协议软件或网络应用软件，甚至网络操作系统，才能实现信息交换。

1．C/S 模式

计算机网络采用客户（Client）/服务器（Server）工作模式进行数据传输，简称 C/S 模式，或客户/服务器模式。客户和服务器是指进行数据传输的两个网络程序或运行了相应网络程序的终端设备。客户/服务器模式所描述的是两个网络程序进程之间的服务和被服务关系。客户程序是数据传输服务的请求方，服务器程序是数据传输服务的提供方，如图 1-8 所示。

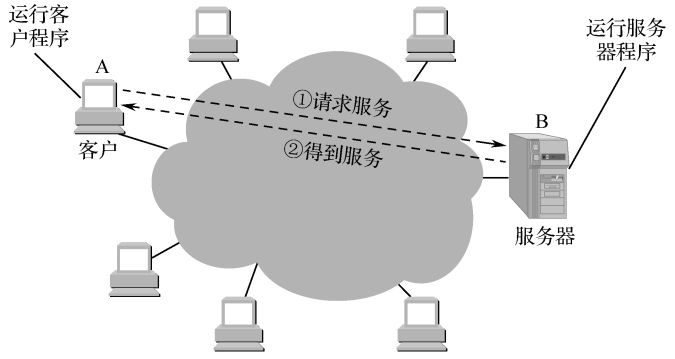


图 1-8　计算机网络的客户/服务器工作模式

客户程序的特点：实现绝大多数的业务逻辑和界面展示，被用户调用运行后，在通信时主动向远地服务器发起服务请求。因此，客户程序必须知道服务器程序的地址，但不需要特殊的硬件和很复杂的操作系统。

服务器程序的特点：专门用来提供某种服务，可同时处理多个远地或本地客户的请求。系统启动后即自动调用并一直不断地运行，被动地等待并接受来自各地的客户的通信请求。因此，服务器程序不需要知道客户程序的地址，但一般需要强大的硬件和高级的操作系统。

2．B/S 模式

随着 Web 技术的发展，在 C/S 模式基础上产生了所谓的 B/S 模式。B/S 全称为 Browser/Server，即浏览器/服务器模式。这种模式也被称为 Web 应用模式，它实际上是将 C/S 应用中的各种客户程序都简化为 Web 浏览器。Browser 指的就是 Web 浏览器程序，它将数据传输给服务器，实现较少的事务逻辑，主要接收服务器传递的数据并进行显示和交互操作。服务器程序将显示和操作代码传递给浏览器，并实现业务系统的主要事务逻辑功能。

B/S 模式的 Web 应用其实也是一种 C/S 应用，只不过客户端使用的是统一协议的浏览器而已，避免了 C/S 模式中网络应用系统修改升级带来的客户程序的重新安装问题。而且传统的 C/S 结构是 2 层结构，客户端直接和数据库连接，这种模式存在较大的安全隐患，而 B/S 模式则易于实现 3 层结构的系统开发，业务逻辑可介于数据库服务器和客户浏览器而在另外的服务器上运行。B/S 与 C/S 的优缺点比较如表 1-1 所示。

表 1-1 B/S 与 C/S 的优缺点比较

模 式	优 点	缺 点
B/S	① 具有分布性特点，可以随时随地进行业务处理； ② 业务扩展简单方便，通过增加网页即可增加服务器功能； ③ 维护简单方便，只需要改变网页，即可实现所有用户同步更新； ④ 开发简单，共享性强	① 较难实现个性化界面设计要求，界面组件扩展性差； ② 操作以鼠标为最基本方式，不适合快速操作的应用； ③ 页面动态刷新，响应速度明显降低； ④ 数据库访问压力较大； ⑤ 功能弱化，难以实现传统模式下的特殊功能要求
C/S	① 客户端实现与服务器的直接相连，没有中间环节，因此响应速度快； ② 客户操作界面设计灵活，容易满足客户自身的个性化要求； ③ 界面组件丰富	① 需要专门的客户端安装程序，分布功能弱，不能实现快速部署安装和配置； ② 由于是针对性开发，业务变更或改变不够灵活，需要重新设计和开发，增加了维护和管理的难度，难以进一步拓展业务； ③ 兼容性差，对于不同的开发工具，相互之间很难兼容，具有较大的局限性。若采用不同工具，需要重新改写程序； ④ 开发成本较高，需要专业水准的技术人员才能完成

B/S 模式的优点是：可在广域网上传输数据，客户端程序无须安装，有 Web 浏览器即可，方便实现地域分散、不同类别的多客户访问，系统维护开销小，比 C/S 有更强的适应范围。缺点是：在速度和安全性上比 C/S 应用模式难控制。

军事信息系统的网络应用与其他网络应用系统一样，主要有 C/S 和 B/S 两种传输模式。各层级的军事信息系统之间的信息传输主要采用 C/S 模式，而面向信息用户的信息使用方式则主要是 B/S 模式。两种模式的网络程序软件开发方法请参考相关书籍。

1.3 计算机网络基本原理

1.3.1 数据交换方式

计算机网络诞生于 20 世纪 50 年代中期，60 年代～70 年代是广域网从无到有并得到大发展的年代；80 年代局域网取得了长足的进步，已日趋成熟；进入 90 年代，一方面广域网和局域网紧密结合使得企业网络迅速发展，另一方面建造了覆盖全球的因特网 Internet；21 世纪已经进入了网络信息社会。互联网是指将多个网络连接形成的更大网络，Internet 是一种互联网，各种大型军事网络也是一种互联网。

现代计算机网络实现数据传输的方式称作“分组交换”，此前还经历了电路交换和报文交换的发展过程。对于图 1-9（a）所示的信息传输任务，它们的大致原理分别如图 1-9（b）、（c）、（d）所示。

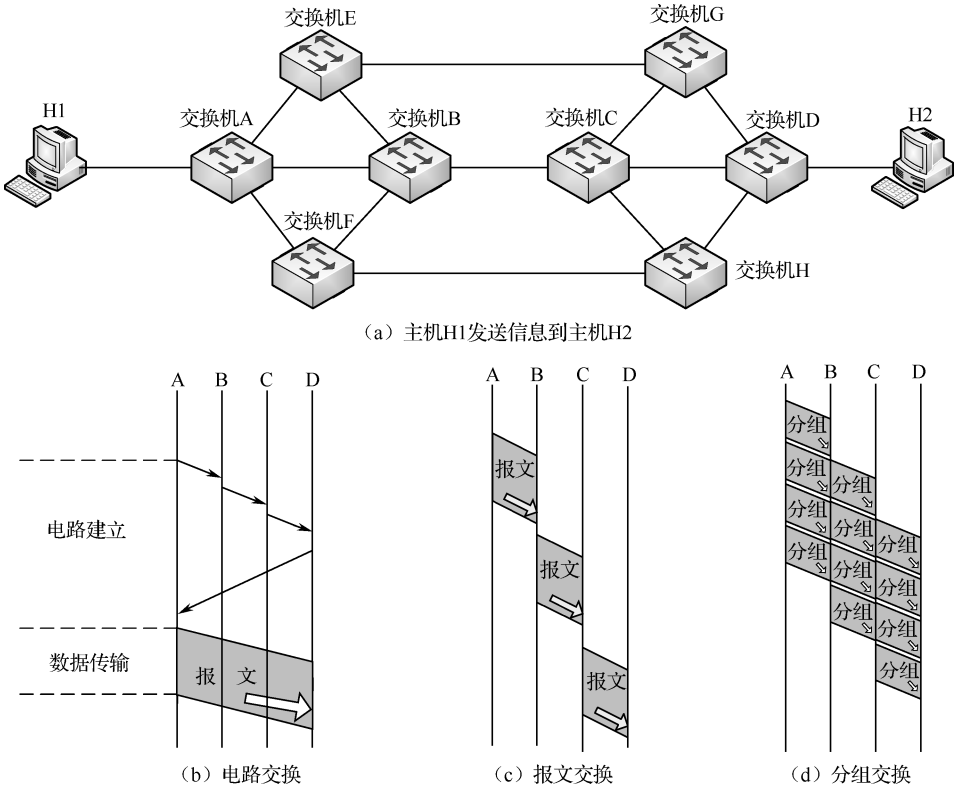


图 1-9　三种交换方式

1．电路交换

电路交换又叫线路交换，是目前电话系统中使用的交换方式。电路交换的主要特点是每次通信前都在通信双方间建立一条临时的、专用的物理传输通路，供通信双方使用，直至通信完毕，交换机内的连线才被拆除。这样，在通信期间这条通路始终由一对用户固定占用，在用户之间提供了完全“透明”的信号通路。典型的例子是电话交换机。电路交换在数据传输过程中要经过电路建立、数据传输和电路拆除三个阶段，如图 1-9（b）所示。

（1）电路建立：在图 1-9（a）中，若 H1 站要与 H2 站连接，典型的做法是，H1 站先向与其相连的 A 节点提出请求，然后 A 节点在通向 D 节点的路径中找到下一个支路。例如 A 节点选择经 B 节点的电路，在此电路上分配一个未用的通道，并告诉 B 它还要连接 C 节点；B 再呼叫 C，建立电路 BC，……，建立电路 BCD，最后，节点 D 完成到 H2 站的连接。这样 A 与 D 之间就有一条专用电路 ABCD，用于 H1 站与 H2 站之间的数据传输。

（2）数据传输：电路 ABCD 建立以后，数据就可以从 A 发送到 B，再由 B 交换到 C，由 C 交换到 D；D 也可以经 C、B 向 A 发送数据。数据传输过程中电路必须始终保持连接状态。

（3）电路拆除：数据传输结束后，由某一方（A 或 D）发出拆除请求，然后逐节点拆除到对方节点。

这种交换方式比较简单，在数据传输的全部时间内用户始终占用端到端的通路，数据传输速度快、传输速率固定，特别适合远距离成批数据传输，建立一次连接就可以传送大量数据；由于无交换机对它进行存储、分析和处理，因而传输用户数据时不必附加用于控制的专门信息，使得传输效率较高。传输时延小、传输延迟固定不变，数据按发送顺序到达，信息编码方法、

信息格式和传输控制程序不受限制。

它的缺点是电路建立时间较长，利用率不高，每次只能一个用户使用，通信成本高；在传输速率、信息格式、编码类型、同步方式、通信规程等方面，通信双方必须完全兼容，这不利于用户终端之间实现互通。当一方用户终端设备忙或交换网负载过重时，可能会出现连接不通的现象。

2．报文交换

报文交换又称包交换，是基于存储转发技术的交换方式。通信双方事先不建立一条物理通路，当发送方有数据要发送时，它把要发送的数据当作一个整体交给中间交换设备，中间交换设备先将报文存储起来，然后根据报文中的目的地址选择一条合适的空闲输出线将数据转发给下一个交换设备，如此循环往复，直至将数据发送到目的节点，如图 1-9（c）所示。因此，端与端之间无须先通过呼叫建立连接。最早采用这种方式的是电报系统。

报文交换的主要特点：报文从源点传送到目的地采用“存储转发”方式，在传送报文时，一个时刻仅占用一段通道。主要优点是：线路利用率较高，在报文交换过程中没有电路的接续过程，也不会把一条线路固定地分配给一对用户使用，而是一条线路可为多个报文进行多路复用，从而大大地提高了线路的利用率；可以起到匹配输入/输出传输速率的作用，而且还能起到防止呼叫阻塞、平滑通信业务量峰值的作用；易于实现各种不同类型终端之间的互通；便于对报文实现多种功能服务，包括速率转换、格式转换、多路转发、优先级处理、差错控制与恢复等。

报文交换的主要缺点：数据信息通过交换网的时延较长，且变化大，这不利于实时或交互型业务；交换机必须具有存储报文的容量和高速分析处理报文的功能，从而增大了交换机的投资费用；报文大小没有通用规定，这就要求各个中间节点必须使用外部存储器来缓存较长的报文；某一报文可能会长时间占用线路，导致报文在中间节点的延迟非常大，从几分钟到几小时不等，而且一旦出错整个报文要全部重发，这使得报文交换不适合交互式数据通信，所以计算机网络中不采用报文交换。为此又引入了分组交换技术。

3．分组交换的提出

传统的电路交换有一个缺点：正在通信的电路中有一个交换机或有一条链路被破坏，则整个通信电路就要中断。如果改用其他迂回电路，必须重新拨号建立连接。虽然电路交换能动态分配传输线路，但用于传输计算机数据的效率很低，并会延误一些时间。计算机网络是 20 世纪 60 年代美苏冷战时期的产物。20 世纪 60 年代初，美国国防部领导的高级研究规划局（Advanced Research Project Agency，ARPA）提出要研制一种具有如下基本特点的生存性强的网络。

（1）网络用于计算机之间的数据传送，而不是为了打电话。

（2）网络能够连接不同类型的计算机，不局限于单一类型的计算机。

（3）所有的网络节点都同等重要，因而大大提高了网络的生存性。

（4）计算机在进行通信时必须有冗余的路由。

（5）网络的结构应当尽可能地简单，同时还能非常可靠地传送数据。

根据以上这些要求，终于设计出了使用分组交换的新型计算机网络。

4．分组交换的原理

分组交换也是一种基于存储转发的交换技术，是报文交换技术的改进，如图 1-9（d）所示。分组交换不像报文交换那样以整个报文为交换单位，而是设法将一份较长的报文分划分成较短的、固定长度的数据段，每一个数据段前面添加上首部构成“分组”，首部带有目的地址和发送地址等固定格式的控制信息，用以指明该分组发往何处。

分组交换网以“分组”作为独立的数据传输单元，依次把各分组发送到接收端；传输过程中各分组之间没有任何联系，既可以断续地传送，又可以经过不同的传输路径；网络中的交换机、路由器等转发设备根据每个分组的首部信息将它们沿着最佳路由发往目的地，接收端收到分组后剥去首部还原成报文。

分组交换的概念并不难理解，它类似于邮寄信件。人们把写好的信放入信封，就如同划分分组；在信封上写上地址，就如同在分组头里放入路由信息；投入邮筒，就如同交换机进行交换，再发往目的地；接到信件后打开阅读，就像拆包后取出信件一样。邮寄信件的过程就如同分组交换过程，只不过分组交换为了把信息更可靠地传给对方，技术上更复杂些而已。

分组交换示意图如图 1-10 所示。分组交换实际上可分以下两种方式。

（1）分组交换数据报方式

如图 1-10（b）所示，每个分组按一定格式附加源与目的地址、分组编号、分组起始、结束标志、差错校验等信息，以“数据报”的分组形式在网络中传输。网络只是尽力地将分组交付给目的主机，整个报文被分解成的各个分组就可能经历不同的路径到达目的站，而且不保证所传送的分组不丢失，也不保证分组能够按发送的顺序到达接收端。所以网络提供的服务是不可靠的，也不保证服务质量。数据报方式一般适用于较短的单个分组的报文。

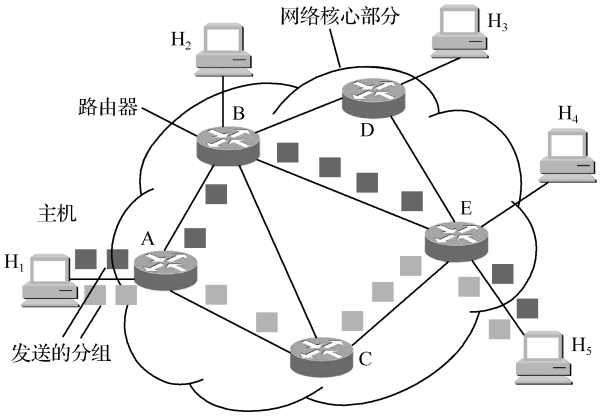
数据报的优点：数据报服务不需要建立连接；每个分组独立选择路由进行转发，当某个节点发生故障时，后续的分组可以另选路由。数据报传送迅速、简单灵活、传输延时小，适用于传输可靠性要求不高、通信子网负载不均衡、需要选择最佳路径的场合。

数据报的缺点：每个分组都要有目的站的全地址，且接收的分组有可能失序。当网络发生故障时，出故障的节点可能会丢失数据，一些路由可能会发生变化；端到端的差错处理和流量控制只由主机负责。每个分组附加的控制信息增多，将增加传输信息的长度和处理时间，增大额外开销。

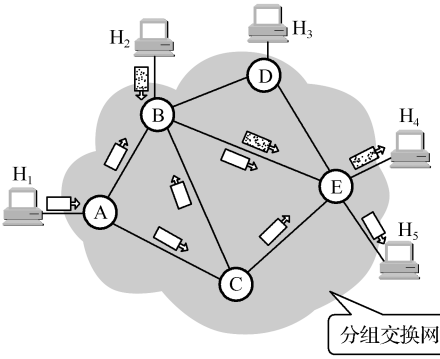
（2）分组交换虚电路方式

如图 1-10（c）所示，虚电路保证所传送的分组按发送的顺序到达接收端。它与分组交换数据报方式的区别主要是在信息交换之前，需要在发送端和接收端之间先建立一个逻辑连接，然后才开始传送分组，所有分组沿相同的路径进行交换转发，通信结束后再拆除该逻辑连接。从现象上来看，传送各分组的这条虚电路似乎与电路交换中建立的那条专用电路一样，但从本质上来看，各分组在每个交换机中仍然需要存储，并在输出线路上排队等待，这就为分组交换虚电路方式有可能提供多种服务（包括排序、流控制和差错控制等）创造了条件。

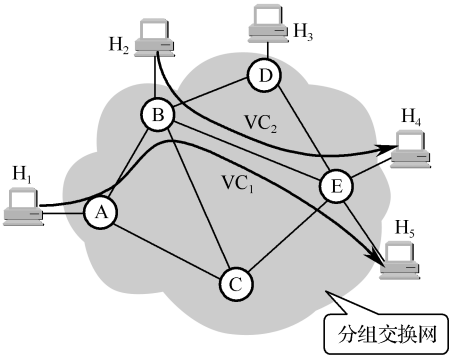
虚电路的优点：虚电路服务是面向连接的，网络能够保证分组总是按照发送顺序到达目的站，且不丢失、不重复，提供可靠的端到端数据传输；目的站地址仅在连接建立阶段使用，每个分组使用短的虚电路号，使分组的控制信息部分的比特数减少，减少了额外开销；端到端的差错处理和流量控制可以由分组交换网负责，也可以由用户主机负责。虚电路服务适用于通信信息量大、速率要求高、传输可靠性要求高的场合。



（a）分组传输示意图



（b）分组交换数据报方式



（c）分组交换虚电路方式

图 1-10　分组交换示意图

虚电路的缺点：虚电路服务必须建立连接；属于同一条虚电路的分组总是按照同一路由进行转发；当节点发生故障时，所有通过出故障的节点的虚电路均不能工作。对信息传输频率高、每次传输量小的用户不太适用，但由于每个分组头只需标出虚电路标识符和序号，所以分组头开销小，适用于长报文传送。

表 1-2 归纳了虚电路服务与数据报服务的主要区别。

表 1-2　虚电路服务与数据报服务的对比

对比的方面	虚电路服务	数据报服务
思路	可靠通信应由网络保证	可靠通信应当由用户主机来保证
连接的建立	必须有	不要
目的站地址	仅在连接建立阶段使用，每个分组使用短的虚电路号	每个分组都有目的站的全地址
分组的转发	属于同一条虚电路的分组均按照同一路由进行转发	每个分组都独立选择路由进行转发
当结点出故障时	所有通过出故障节点的虚电路均不能工作	出故障的节点可能会丢失分组，一些路由可能会发生变化
分组的顺序	总是按发送顺序到达目的站	不一定按发送顺序到达目的站

续表

对比的方面	虚电路服务	数据报服务
端到端的差错处理和流量控制	可以由分组交换网负责，也可以由用户主机负责	由用户主机负责

5．分组交换的特点

由于分组长度固定且较短（如每个分组为 512 比特），又具有统一的格式，就便于交换机存储、分析和处理。分组进入交换机进行排队和处理只需停留很短的时间，一旦确定了新的路由，就立刻被转发到下一个交换机或用户终端。

分组交换时动态分配带宽，通信双方都不能长时间独占通路，所以带宽利用率高。在传输过程中，分组交换机还对每一个分组提供一定程度的差错控制，传输可靠性较高。另外，分组交换能实现多路通信。由于这些原因，分组交换技术是计算机网络中使用最广泛的一种交换技术，适用于中等或大量数据的传输。

（1）分组交换的优点

① 高效：动态分配传输带宽，对通信链路逐段占用，可以同时和多个用户终端进行通信。

② 灵活：以分组为传送单位和查找路由，能够实现不同速率、码型和传输控制规程终端间的互通，为不同种类的计算机终端相互通信提供方便。

③ 迅速：不必先建立连接就能向其他主机发送分组，传输时延较小；充分使用链路的带宽。

④ 可靠：完善的网络协议，具有差错控制功能；自适应的路由选择协议使网络生存性高。

（2）分组交换带来的问题

分组在各节点存储转发时需要排队，这就会造成一定的时延；分组必须携带首部（里面有必不可少的控制信息），也造成了一定的开销。分组交换过程中还需传输一些非用户数据的控制分组，用来进行差错控制和流量控制等，也要消耗一定的网络通信能力。除此之外，分组交换网中的交换机、路由器等网络设备对每个分组都需要封装、拆分、处理，从而为分组提供传输路由，为数据终端设备提供速率、格式、码型和规程等的变换，为网络的维护管理提供必需的报告信息等，其性能对网络通信能力影响较大。

6．分组交换的发展

传统的交换机有一定的开销，传输速率不能满足对实时性要求高的应用要求，因此在分组交换的基础上发展了帧中继、ATM 等高速交换技术。

帧中继技术是在开放系统互联参考模型数据链路层上，用简化的方法传送和交换数据单元的一种技术。帧中继传送数据信息所使用的传输链路是逻辑连接，在一个物理连接上可以复用多个逻辑连接。应用这一机理，可实现带宽的复用和动态分配。采用帧中继技术实现的数据通信网称为帧中继网，通常由帧中继接入设备、帧中继交换设备、中继电路和网络管理设备等组成。

ATM 是异步传输模式的简称，又称为信元中继交换。ATM 是一种快速分组交换技术，吸取了电路交换和分组交换的长处，使用固定长度（53 字节）的短信元作为分组单位，便于采用高速硬件对信头进行识别和交换处理，使传输控制大大简化，比较适合声音、视频等多媒体数据的通信。

1.3.2 网络体系结构

计算机网络是由多种计算机和各类终端通过通信线路连接起来的复合系统。在这个系统中，由于计算机型号不一，终端类型各异，加之线路类型、连接方式、同步方式、通信方式不同，给网络中各节点的通信带来了许多不便。不同计算机系统之间进行协同通信十分复杂。

因此，计算机网络中的数据交换必须遵守事先约定好的规则。这些规则明确规定所交换的数据的格式及有关的同步问题（同步含有时序的意思）。为进行网络中的数据交换而建立的规则、标准或约定称为网络协议（Network Protocol）。网络协议的组成要素有 3 个。

（1）语法：数据与控制信息的结构或格式。规定怎么做（how to do）。

（2）语义：需要发出何种控制信息、完成何种动作及做出何种响应。规定做什么（what to do）。

（3）同步：事件实现顺序的详细说明。规定何时做（when to do）。

计算机网络协议是分层的。层次划分的思想：按照信息的流动过程将网络的整体功能分解为一个个功能层，不同计算机上的同等功能层之间采用相同的协议，同一计算机上的相邻功能层之间通过接口进行信息传递，从而将网络这个庞大的、复杂的问题划分成若干较小的、简单的、比较易于研究和处理的问题。采用分层设计方法使得每个协议的设计、分析、编码和测试都比较容易。

计算机网络中，分层、协议和层间接口的集合被称为计算机网络体系结构。显然，网络体系结构包含三个问题：①分层与功能问题，即网络应该具有哪些层次？每一层的功能是什么？②协议问题，即通信双方的数据传输要遵循哪些规则？③服务与接口问题，即各层之间的关系是怎样的？它们如何进行交互？

为阐释计算机网络的原理，一般将其体系结构分为五层，每一层完成特定的功能。这五层分别称为物理层、数据链路层、网络层、运输层和应用层，如图 1-11 所示。

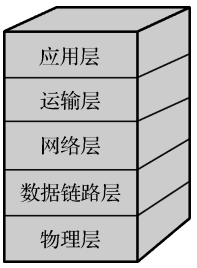


图 1-11　计算机网络体系结构模型

1．物理层

物理层的任务就是在通信信道上透明地、正确地发送和接收二进制比特流。在物理层上所传数据的单位是比特（bit）。它要考虑用多大电压表示二进制的“1”，用多大电压表示二进制的“0”。还要考虑物理接口的机械、电气标准，如在任何地方买的水晶头都应该能够插入一个以太网网卡中，这就是因为它们遵守了相同的物理层协议。同时，物理层还要考虑各种物理传输介质问题，但物理层并不是指连接计算机的具体的物理设备或具体的传输媒体。

物理层的作用就是确定与传输媒体接口的一些特性。

（1）机械特性：指明接口所用接线器的形状和尺寸、引线数目和排列、固定和锁定装置。
（2）电气特性：指明在接口电缆的那条线上出现的电压的范围。
（3）功能特性：指明某条线上出现的某一电平的电压表示何种意义。
（4）规程特性：指明不同功能的各种可能事件的出现顺序。

2．数据链路层

数据链路层的任务是在两个相邻设备间的线路上无差错地传输数据，保证将源端主机物理层的数据帧准确无误地传送到目的主机的物理层。帧是指需传送的数据和必要的控制信息的集合，其中控制信息包括同步信息、地址信息、差错控制及流量控制信息等。数据链路层的帧使用物理层提供的比特流传输服务来到达目的主机数据链路层。为了保证数据传输的准确无误，数据链路层还负责物理拓扑、差错控制和流量控制等。

数据链路层必须解决帧定界、透明传输和差错检测三个基本问题。
（1）帧定界：使收方能从收到的比特流中准确地区分出一个帧的开始和结束位置。
（2）透明传输：使得不管所传数据是什么样的比特组合，都应当能够在链路上传送。
（3）差错控制：主要包括差错检测和差错纠正，旨在降低传输的比特差错率。

3．网络层

网络层位于层次模型的第三层，它利用其下两层提供的服务来实现传输层的通信，将数据包从源网络发送到目的网络。网络层为主机之间提供逻辑通信。简单地讲就是：计算路由、定义网络的地址。在网络层，数据传送的单位是分组或包。网络层检查网络拓扑，以决定传输的数据包的最佳路由、转发数据包。选择“最佳路由”，是指网络层通过运行路由协议来计算到达目的地的最佳路由，找到数据包应该转发的下一个网络设备。网络层同时还要处理拥塞控制和 QoS 问题。网络层设备的每一个接口都有一个唯一的物理层地址，称为逻辑地址，这个地址是全球唯一的。对于由广播信道构成的网络，路由问题很简单，甚至可以没有。

4．运输层

运输层位于层次结构的第四层，为应用进程之间提供端到端的逻辑通信。运输层向应用层的进程提供有效的、可靠的服务。信息的传送单位是报文，由运输层以复用和分用的形式加载到网络层。它一般包括将应用层发往网络层的数据分段或将网络层发往应用层的数据段合并，用于建立端到端的连接，主要是建立逻辑连接以传送数据流，将数据报文从一台主机正确地传送到另一台主机，从而保证传输的正确性。

运输层为面向通信部分的最高层。运输层同时也是用户功能中的最低层，向它上面的应用层提供服务。运输层以上的各层面向应用进程，而运输层以下的各层面向数据传输。正因为如此，运输层就成为计算机网络体系结构中非常重要的一层。

5．应用层

应用层是计算机网络体系结构中的最高层，主要用于处理平常广泛使用的网络应用，如 HTTP、FTP、DNS 和 SMTP 等。需要注意的是，应用层协议并不是解决用户各种具体应用的协议。

从上可见，计算机网络体系结构具有这样的特点：以功能作为划分层次的基础，每一层都

有各自的特定功能；第 n 层的实体在实现自身定义的功能时，只能使用第 n−1 层提供的服务；第 n 层在向第 n+1 层提供服务时，此服务不仅包含第 n 层本身的功能，还包含由下层服务提供的功能；仅在相邻层间有接口，且所提供服务的具体实现细节对上一层完全屏蔽。

分层的体系结构带来的好处主要体现在以下方面。

（1）各层之间相对独立。某一层并不需要知道它的下一层是如何实现的，而仅需要知道该层间的接口（即界面）所提供的服务。由于每一层只实现一种相对独立的功能，因而可将一个难以处理的复杂问题分解为若干个较容易处理的更小一些的问题。这样，整个问题的复杂程度就下降了。

（2）灵活性好。当任何一层发生变化时（如技术的变化），只要层间接口关系保持不变，则这层以上或以下的各层均不受影响。

（3）易于实现和维护。这种结构使得实现和调试一个庞大而又复杂的系统变得易于处理，因为整个系统已被分解为若干个相对独立的子系统。

（4）易于标准化。因为每一层的功能和所提供的服务均已有精确的说明。

1.3.3 TCP/IP 协议模型

APARNET 是最早出现的计算机网络之一，现代计算机网络的很多概念与方法都是从它的基础上发展起来的。20 世纪 60 年代，美国国防部高级研究计划署（APAR）提出 APARNET 研究计划，希望它的很多宝贵的主机、通信控制处理机与通信线路在战争中一旦被部分破坏，其他部分还能正常工作；同时，希望适应从文件传送到实时数据传输的各种应用需求。因此，它要求一种灵活的网络体系结构，实现异型网络的互连与互通。这就导致了网络协议 TCP/IP 的出现。

TCP/IP 参考模型是一种分层结构。它是由基于硬件层次上的四个概念性层次构成，即网络接口层、网际层、传输层和应用层。TCP/IP 模型是 1974 年首先定义的，自 1983 年成为因特网的事实标准以来，广泛用于校园网等各种互连网络，并已融入 Windows 等各种操作系统中。

TCP/IP 实际上是一组协议，是当前互联网和局域网所使用的最流行的网络“标准”。虽然它不是国际标准，但这个协议的应用量大且广，已经成为事实上的国际标准或工业标准。图 1-12 描述了 TCP/IP 体系结构的参考模型，图 1-13 表示了 TCP/IP 参考模型与国际标准化组织制定的 OSI（Open System Interconnect）参考模型在功能上的对应关系。

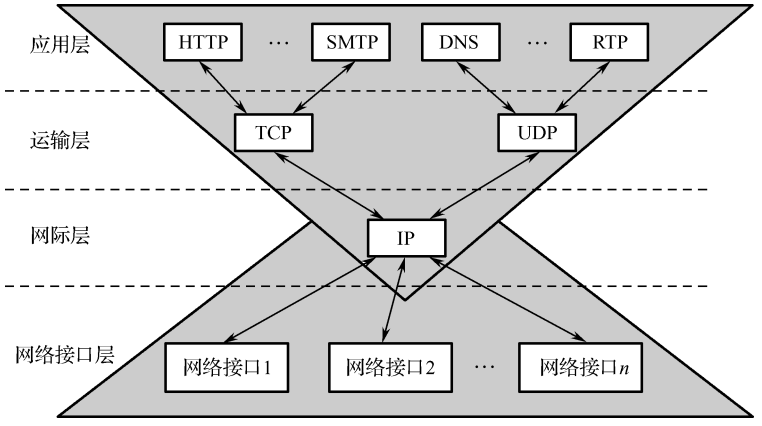


图 1-12 TCP/IP 体系结构

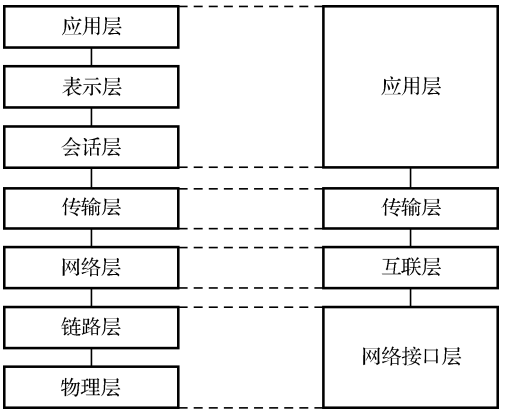


图 1-13　TCP/IP 参考模型与 OSI 参考模型的对应关系

OSI 的主要问题：定义复杂、实现困难，有些功能在每一层重复出现，效率低下。而 TCP/IP 则具有以下特点。

（1）开放的协议标准，可以免费使用，并且独立于特定的计算机硬件和操作系统。

（2）独立于特定的网络硬件，可以运行在局域网和广域网，更适用于因特网中。

（3）统一的网络地址分配方案，使整个 TCP/IP 设备在网络中都拥有唯一的地址。

（4）标准化的高层协议，可以提供多种可靠的用户服务。

下面介绍 TCP/IP 参考模型各层中的有关协议及其作用。

1．网络接口层（Network Interface）

网络接口层在 TCP/IP 参考模型中并无真正描述，相当于 OSI 中最低两层即数据链路层和物理层的功能。其作用是将上层的协议和下层的网络硬件隔离开来，实现不同类型的物理网络的传输介质都能收发数据包。正是这一点使得 TCP/IP 网络具有相当的灵活性，底层传输不依赖于某种特定的网络硬件，也不依赖于某种特定的数据帧格式和传输介质。

网络接口层代表任何一个能通过物理地址传输数据报的通信系统，从而将 IP 数据报再包装成该通信系统可以传输的数据帧（Frame），通过不同的驱动程序来支持各种类型的网络硬件和组网方式，如 Ethernet（以太网）、Token Ring（令牌网）、Frame Relay（帧中继）和 ATM 等。

2．网络层（Internetwork Layer）

网络层又称 IP 层、网际层、互联层，与传输层建立两台计算机的端对端的连接不同，网络层负责 IP 寻址、数据包的分裂和重组，实现在任何两个子网之间“无连接”地传输数据报。通过 IP 协议和 IP 地址，屏蔽了不同的物理网络（如以太网、令牌环网等）的帧格式、地址格式等各种底层物理细节，使得各种物理网络的差异性对上层协议不复存在。

（1）IP 协议的主要功能

① 将运输层传递来的数据段定义为 IP 数据报。

IP 协议由上层接收 TCP 数据段后，添加自己的头标以形成统一的 IP 数据报（数据分组，是最基本的传输单元）。

② 为 IP 数据报选择可到达接收主机所在网络的路由。

IP 协议只负责解决 IP 数据报在物理网络之间的路由选择，即在各台主机与路由器中建有

路由表，用以指明两部分内容：各主机的网络地址及其对应的下一个应传输的路由器或网络的地址。由于在同一网络中主机的网络地址相同，从而可以大大减小路由表的规模。

③ 确定网间寻址方案。

互连网络中的每一个网络（子网）和计算机都有自己的 IP 地址，但每个具体网络传输数据所使用的物理地址是不一样的。IP 协议在具体网络接口协议的配合下，可以将 IP 地址转换成具体网络和计算机的物理地址，或进行逆向转换。

ARP 地址解析协议（Address Resolution Protocol）就用来实现 IP 地址向其对应物理地址的转换，如将一台主机的 IP 地址解析成以太网网卡的 MAC 地址，而 RARP 逆向地址解析协议（Reverse Address Resolution Protocol）则实现逆地址转换。这两个协议也可看成网络层与网络接口层之间的接口层协议。

④ 将 IP 数据报传输到网络接口层。

为了实现 IP 数据报在同一网络中的传输，需要将它传输给下面的网络接口层（在这一层再转换成对应网络的数据链路层中的数据帧）。

⑤ 必要时对 IP 数据报进行分片和重组。

分片是指 IP 数据报的尺寸大于将发往网络的 MTU（最大传送单元）值时，路由器将 IP 数据报分成若干较小的部分的过程，如图 1-14 所示。每个分片由报头区和数据区两部分构成。每个分片经过独立的路由选择等处理过程后最终到达目的主机。

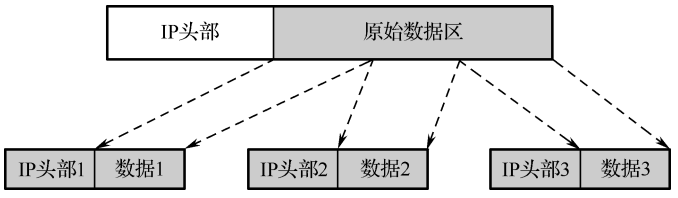


图 1-14　IP 数据报分片示意图

目的主机在接收到所有分片后，对分片进行重新组装，如图 1-15 所示。路由器不需要对分片进行重组，也不可能对分片进行重组。

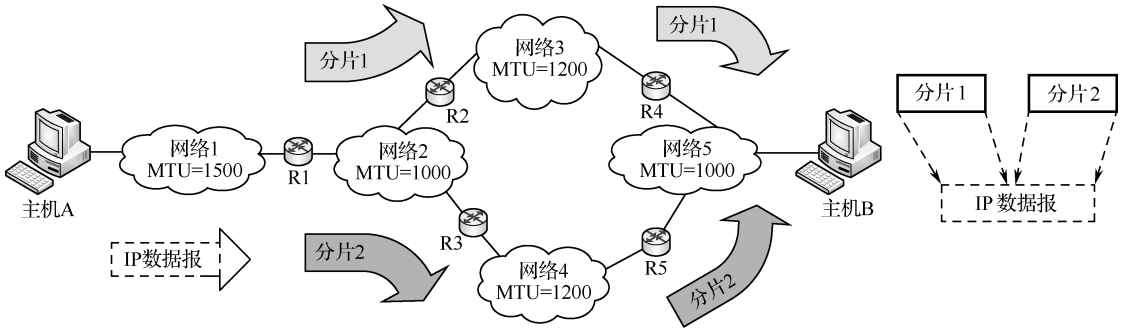


图 1-15　IP 数据报分片的传输及重组示意图

网络层还使用网际控制消息协议（Internet Control Message Protocol，ICMP）来检测目标网络、站点或端口能否到达，目标主机或网络互联设备根据 ICMP 协议向发送端发送差错报文来报告 IP 数据包传送中的错误信息，从而实现信息传输管理和网络维护。Ping 程序就是用 ICMP 协议检测某台主机的典型例子。ICMP 协议也可看成 IP 协议的一部分。

（2）IP 协议的特点

① IP 协议向 TCP 层提供无连接的数据报传输机制，对数据分组进行“尽力传递”。即只将数据分组传往信宿机，无论传输正确与否，不做验证，不发确认，也不保证分组的顺序正确，数据传输的可靠性在 TCP 层体现，这样就提高了 TCP/IP 的效率。尤其是当低层网络技术可靠性高时，TCP/IP 的效率更加可观。

② IP 协议是点到点的。它是 TCP 协议层实现端到端传输的基础。所谓端到端传输即指初始信源机上的 TCP 实体与信宿机的对等 TCP 实体进行直接通信，仿佛彼此之间拥有一条直接线路。

（3）IP 协议的格式

目前广泛使用的是 IPv4 版，据其形成的 IP 数据报格式如图 1-16 所示。

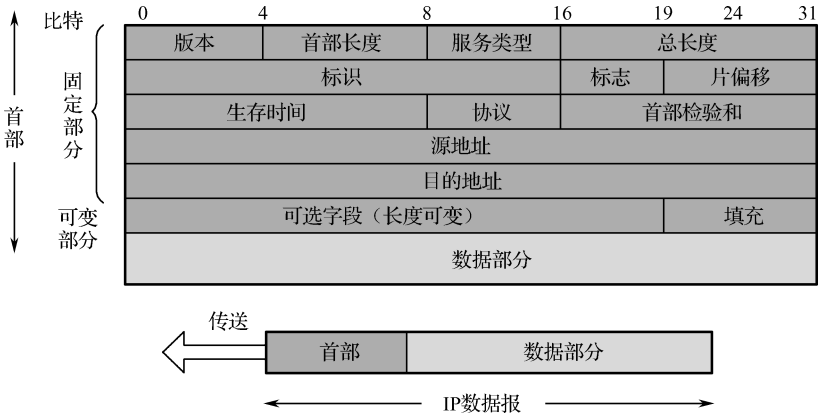


图 1-16　IP 数据报及其首部的格式

一个 IP 数据报由首部和数据两部分组成。首部的前一部分是固定长度的，共 20 字节，是所有 IP 数据报必须具有的，固定部分的后面是一些可选字段，其长度是可变的。IP 数据报有两层含义：第一指 IP 层的无连接数据报传输机制和 IP 层无连接服务；第二指 IP 层传输的数据单元及其格式。数据报机制通过数据报格式体现。

从图 1-16 可见，IP 数据报的首部包含了发送端和接收端的主机的 IP 地址，这样就可以建立计算机到互联网的一个连接。IP 地址唯一地标识了网络上的计算机。

其中：

① 版本——占 4bit，指 IP 协议的版本，目前的 IP 协议版本号为 4（即 IPv4）。

② 首部长度——占 4bit，可表示的最大数值是 15 个单位（一个单位为 4 字节），因此 IP 的首部长度的最大值是 60 字节。

③ 服务类型——占 8bit，用来获得更好的服务，这个字段很少被人们使用。

④ 总长度——占 16bit，指首部和数据之和的长度，单位为字节，因此数据报的最大长度为 65535 字节。总长度必须不超过最大传送单元 MTU。

⑤ 标识（identification）——占 16bit，它是一个计数器，用来产生数据报的标识。

⑥ 片偏移（12bit）：指出较长的分组在分片后某片在原分组中的相对位置。片偏移以 8 字节为偏移单位。

⑦ 生存时间（8bit）——记为 TTL（Time To Live），是数据报在网络中的寿命，其单位为秒。

⑧ 协议（8bit）——指出此数据报携带的数据使用何种协议，以便决定目的主机的 IP 层将数据部分上交给哪个处理过程。

⑨ 首部检验和（16bit）——只检验数据报的首部，不包括数据部分。这里不采用 CRC 检验码而采用简单的计算方法。

⑩ 源地址和目的地址——表示发送端和接收端主机的 IP 地址，各占 4 字节。32 位的 IP 地址一般用 4 个十进制数值表示，数值间用“．”隔开。IP 地址就是给每个连接在因特网上的主机（或路由器）分配一个在全世界范围唯一的 32bit 的标识符。因特网上的 IP 地址由因特网名称与数字地址分配机构（Internet Corporation for Assigned Names and Numbers，ICANN）进行分配。

3．运输层（Transport Layer）

运输层又称传输层，运输层为应用进程之间提供逻辑通信，而网络层为主机之间提供逻辑通信。运输层为上层应用程序建立和提供端到端的通信连接，它从应用层的有关应用程序接收数据再发送给下面的网络层。

根据应用不同，运输层需要两种不同的运输协议，即面向连接的 TCP 传输控制协议和无连接 UDP 用户数据报协议。运输层向高层用户屏蔽了下面通信子网的细节（如网络拓扑、协议），它使应用进程看见的就好像是在两个运输层实体之间有一条端到端的逻辑通信信道，这条逻辑通信信道对上层的表现却因运输层使用的不同协议而有很大的差别。当运输层采用面向连接的 TCP 协议时，该逻辑通信信道就相当于一条全双工的、可靠的信道，尽管下面的网络是不可靠的（即只提供尽最大努力服务）。当运输层采用无连接的 UDP 协议时，这种逻辑通信信道则是不可靠的信道。

（1）TCP 传输控制协议

TCP 传输控制协议（Transmission Control Protocol）在发送第一个数据包前，首先向接收方发送一个特定的命令，在发送方和接收方之间建立一个一对一的、端对端的“虚电路”连接。然后陆续传送真实数据，当所有的数据传送完毕后，连接根据命令而自动解除。TCP 协议提供连接的确认、数据包发送/接收顺序的控制及出错重传等机制，以保证数据包按照特定顺序陆续正确传输。这些机制是借助如表 1-3 所示的 TCP 报文格式实现的。

表 1-3　TCP 报文格式

<table>
<tr><td colspan="8">16 位源端口号</td><td>16 位目的端口号</td></tr>
<tr><td colspan="9">32 位序号</td></tr>
<tr><td colspan="9">32 位确认序号</td></tr>
<tr><td>4 位首部长度</td><td>保留 6 位</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>16 位窗口大小</td></tr>
<tr><td colspan="8">16 位检验和</td><td>16 位紧急指针</td></tr>
<tr><td colspan="9">可选项</td></tr>
<tr><td colspan="9">数据</td></tr>
</table>

TCP 协议的主要特性与功能如下。

① TCP 的编号与确认。

序号：TCP 对所要传送的报文中的每一字节编一个序号，用来标识从 TCP 发送端向接收

端发送的数据字节流，它表示在这个报文段中的第一个数据字节。如果将字节流看作两个应用程序间的单向流动，则 TCP 用序号对每个字节进行计数。在建立连接时，双方要商定初始序号。

确认：TCP 的确认是对接收到的数据的最高序号（收到的数据流中的最后一个序号）进行确认。但返回的确认序号是已收到的数据的最高序号加 1，即确认序号表示期望下次收到的第一个数据字节的序号。

TCP 为应用层提供全双工服务。因此，连接的每一端必须保持每个方向上的传输数据序号。TCP 首部中的确认序号表示发送方已成功收到字节，但不包含确认序号所指的字节。

TCP 的确认是对一段报文的确认，而不是对一个字节的确认，这是因为：假设用户只发一字节信息，加上 20 字节的首部后，得到 21 字节长的 TCP 报文段。再加上 20 字节的 IP 首部，形成 41 字节长的 IP 数据报。在接收端 TCP 发出确认，构成的数据报是 40 字节长的。若用户要求远地主机回送这一字符，则用户仅发一个字符，线路上就需传送总长度为 162 字节共 4 个报文段（包括用户端对回送字符的确认）。当线路带宽并不富裕时，这种传送方法效率很低。

② 实现进程连接。

TCP 协议可以在两个网络通信进程间同时建立多个连接。通过定义特定的“端口”，对不同通信进程的数据包进行标识。也就是说，端口是用来区分应用层的不同进程的。端口值介于 0 和 65 535 之间。每个 TCP 段都包括源端和目的端的端口号，用于寻找发送端和接收端的应用进程。这两个值加上 IP 首部的源端 IP 地址和目的端 IP 地址可唯一确定一个 TCP 连接。

TCP 连接的建立都采用客户/服务器方式。主动发起连接建立的应用进程叫作客户（Client），被动等待连接建立的应用进程叫作服务器（Server）。TCP 连接的建立过程如图 1-17 所示。

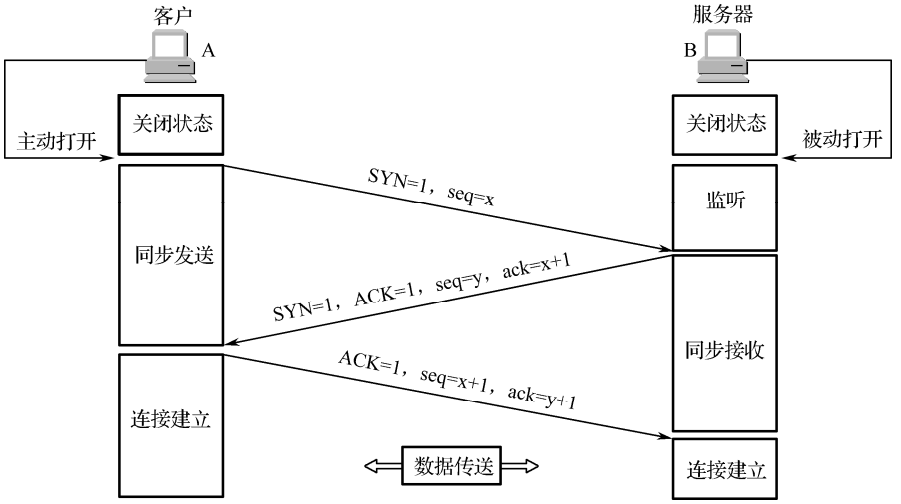


图 1-17　TCP 连接的建立过程

A 的 TCP 向 B 发出连接请求报文段，其首部中的同步位 SYN=1，并选择序号 seq=x，表明传送数据时的第一个数据字节的序号是 x。B 的 TCP 收到连接请求报文段后，如果同意，则发回确认。B 在确认报文段中应使 SYN=1，使 ACK=1，其确认号 ack=x+1，自己选择的序号 seq=y。A 收到此报文段后向 B 给出确认，其 ACK=1，确认号 ack=y+1。此时 A 的 TCP 通知上层应用进程连接已经建立。B 的 TCP 收到主机 A 的确认后，也通知其上层应用进程 TCP 连接已经建立。只有确认序号有效的标志 ACK 为 1 时确认序号字段才有效。一旦一个连接建立

起来，ACK 标志总会被设置为 1。

TCP 连接的释放过程如图 1-18 所示。之所以 A 在最后还要定时等待一定时间，主要是为了保证 A 发送的最后一个 ACK 报文段能够到达 B。同时，避免“已失效的连接请求报文段”出现在本连接中，使本连接持续的时间内所产生的所有报文段都从网络中消失。

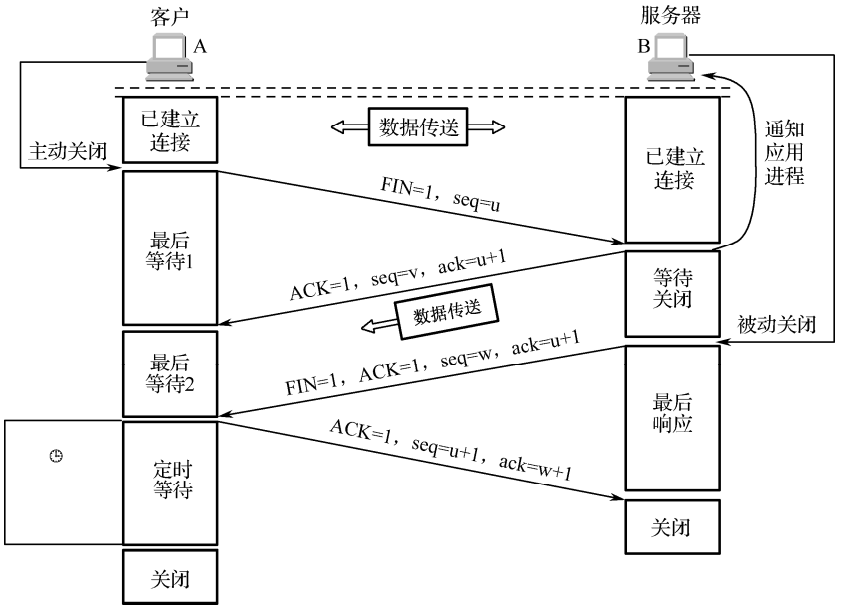


图 1-18　TCP 连接的释放过程

连接建立为什么要采用“三次握手”？这主要是为了防止已失效的连接请求报文段突然又传送到了进程 B，因而产生错误。

假设进程 A 发出连接请求，但因连接请求报文丢失而未收到确认。进程 A 于是再重传一次。后来收到了确认，建立了连接。数据传输完毕后，就释放了连接。进程 A 共发送了两个连接请求报文段，其中的第二个连接请求报文到达了进程 B。这种情况下假设：进程 A 发出的第一个连接请求报文段并没有丢失，而是在某些网络节点滞留的时间太长，以致延误到在这次的连接释放以后才传送到进程 B。本来这是一个已经失效的报文段。但进程 B 收到此失效的连接请求报文段后，误认为是进程 A 又发出一个新的连接请求，于是就向进程 A 发出确认报文段，同意建立连接。

这样，进程 A 由于并没有要求建立连接，因此不会理睬进程 B 的确认，也不会向进程 B 发送数据，但进程 B 以为连接建立了，并一直等进程 A 发来数据。进程 B 的资源就这样白白浪费了。采用三次握手的方法可以防止上述现象的发生。在这种情况下，进程 A 不会向进程 B 发出确认。进程 B 收不到确认，连接就建立不起来。

③ 形成数据分组（划分数据段）。

TCP 将从上层应用程序或进程收到的字节形式的数据流（Data Stream）按既定规则分成若干个数据段（Segment，数据分组）。TCP 给每个数据段加上自己的首部后传给下面网络层的 IP 协议，IP 再给数据段加上自己的首部以形成 IP 数据报（数据分组）。

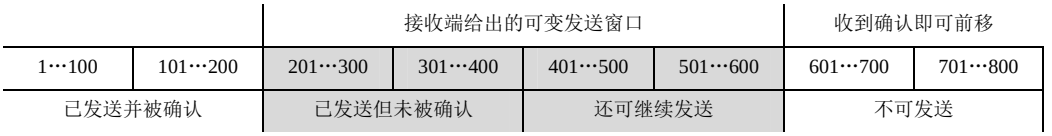
④ 实现流量控制。

流量控制就是让发送方的发送速率不要太快，既要让接收方来得及接收，又不要使网络发生拥塞。TCP 的流量控制机制由连接的每一端通过声明的窗口大小来提供，通过可变发送窗口

的大小进行流量控制。窗口大小为字节数，起始于确认序号字段指明的值，这个值是接收端期望接收的字节数。窗口大小的单位是字节，因而窗口最大为 65 535 字节。在 TCP 报文段首部的窗口字段写入的数值就是当前设定的接收窗口数值。

发送窗口在连接建立时由双方商定。但在通信的过程中，接收端可根据自己的资源情况随时动态调整自己的接收窗口（可增大或减小），然后告诉对方，使对方的发送窗口和自己的接收窗口一致。因此，TCP 是一个没有选择确认或否认的滑动窗口协议。

TCP 滑动窗口的概念示例：



利用可变窗口大小进行流量控制示例（初始连接建立时 B 告诉 A 发送窗口为 400 字节）：

⑤ 保证数据段可靠传输。

计算机网络依靠网络层的 IP 协议和运输层的 TCP 协议共同实现可靠的分组交换。其中，IP 协议保证 IP 数据报的路由选择，而 TCP 协议保证数据段分组的可靠传输。

由于网络层不能保证 IP 数据报的顺序传递和不重、不丢，因此，由运输层的 TCP 通过下列机制来保证数据段的可靠传输。

一是 TCP 协议利用对 TCP 首部和 TCP 数据的“检验和”判断数据段传输过程中是否出错。检验和的字段值由发送端计算和存储，由接收端进行验证。

二是当 TCP 由发送方发送数据段时，启动计算机内部的时钟计时器，接收方收到正确无误的数据段后即返回一个 ACK 确认接收应答信息，否则返回一个 NAK 否认接收应答信息，表明数据段校验错；如果发送方在计时器时限内收到 NAK 信息，或超过时限后仍未收到 ACK 确认信息，TCP 均自动重发。

三是 TCP 在发出的数据段中通过若干标识位来标记数据段的顺序，接收方发现有重复的数据段则删除之；四是为了避免网络上出现过多的无效数据段，TCP 还采用自动调整时限值的方法来进行自动延时调整，即在网络信息传输量较大时自动增加时限值；反之，则自动减小时限值。

（2）用户数据报协议

用户数据报协议（User Datagram Protocol，UDP）提供一对一或一对多的通信服务，它不

提供连接确定、数据包顺序控制及出错重传等机制，所以传输的数据有可能是不可靠的。但它简单、效率高，适合传送对数据传输可靠性要求不高、记录长度固定的数据（如低质量的视频图像数据）或较短的（信息、指令）信息。

UDP 和 TCP 的比较如下。

① TCP 协议没有确保最小传输速率，不允许发送进程按自己的意愿以任何速率发送，必须受 TCP 协议中拥塞控制机制的制约，它可能迫使发送方以较低的平均速率发送。

② TCP 协议并不保证数据传输时间的长短。

③ UDP 协议没有拥塞控制机制，同时有最低速率要求，UDP 也不提供时延保证（通常用于实时应用，可以忍受数据丢失）。

4．应用层（Application Layer）

应用层向用户（用户程序或进程）提供各种网络应用协议及各自对应的应用程序。应用层的协议是多样化的，这也说明计算机网络的应用是多样化的。下面简单举例说明。

（1）Telnet 远程终端协议

Telnet 远程终端协议（Remote Terminal Protocol）是提供远程终端连接服务的标准协议，它让用户的计算机作为远程连接到某台服务器上的仿真终端。

（2）文件传送协议

文件传送协议（File Transfer Protocol，FTP）使某台计算机上的用户可以从另一台服务器上取得文件，或把文件传给另一台服务器。

（3）超文本传输协议

超文本传输协议（Hyper Text Transport Protocol，HTTP）是 WWW 浏览器（Browser）和 WWW 服务器之间用于分布式协作超文本信息系统的、通用的、面向对象的应用层通信协议，用于保证正确传输超文本文档，还确定传输文档中的每一部分的显示顺序。

B/S 模式的 Web 应用程序就是采用 HTTP 进行数据传输的，而 HTTP 是基于 TCP/IP 协议族运行的。所以，无论是 IE 浏览器还是其他浏览器程序，其内部都集成了 HTTP 的功能，并调用计算机操作系统中已集成安装的 TCP/IP 功能，如图 1-19 所示。HTTP 协议层之上的 Web 应用层也还需要多种协议，如 HTML/Javascript/HTC/xml/pic 等，以便支持 Web 页面显示和人机交互。这些协议规定的内容和用法请参考其他书籍。

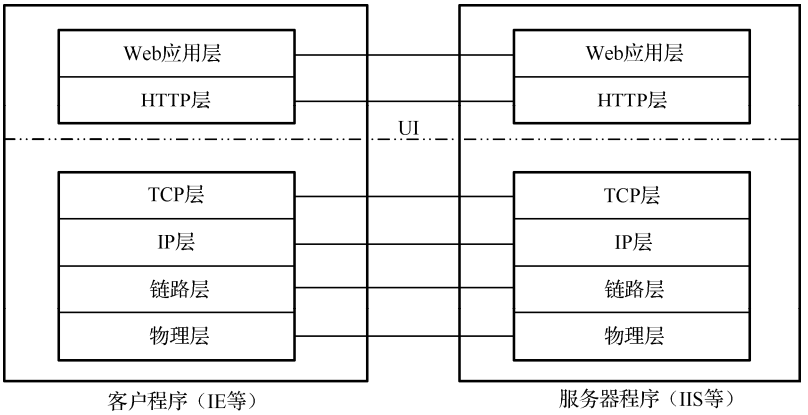


图 1-19　Web 应用的数据传输协议层次

（4）简单网络管理协议

简单网络管理协议（Simple Network Management Protocol，SNMP）与运输层的 UDP 相配合，用于管理 IP 网间节点、互连的集线器、交换机和计算机等通信设备。

（5）动态主机配置协议

在使用 TCP/IP 网络时，每一台计算机都必须有一个唯一的 IP 地址，计算机之间依靠该 IP 地址进行通信。因而，IP 地址的管理、分配与设置就显得非常重要。如果网络管理员手动为每一台计算机设置 IP 地址，会特别麻烦并容易出错。使用动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）就可以解决这个问题。DHCP 服务器可以自动为局域网中的计算机分配 IP 地址及 TCP/IP 设置。

DHCP 是一种客户机/服务器协议，该协议简化了客户机 IP 地址的配置和管理工作及其他 TCP/IP 参数的分配。网络中 DHCP 服务器以自动的方式给运行 DHCP 的客户机分配 IP 地址和相关的 TCP/IP 配置信息。DHCP 服务器拥有一个 IP 地址池，当任何启用 DHCP 的客户机登录到网络时，都可从它那里租借到一个 IP 地址。因为 IP 地址是动态的（租借）而不是静止的（永久分配），不使用的 IP 地址就自动返回地址池，供再次分配，可有效提高 IP 地址空间的利用率。

DHCP 服务器是安装了 DHCP 网络组件的一台计算机，运行有 TCP/IP 协议，并由管理员为其配置 IP 地址、子网掩码、默认网关等内容。DHCP 服务器必须使用静态 IP 地址，为客户机分配的 IP 地址也可以是固定的 IP 地址。

（6）域名系统协议

域名是一种使用字母和数字组成的符号（即名字）来标识互联网上主机的地址表示形式，便于人们的理解和记忆，它与主机的 IP 地址一一对应。由于互联网在低层是依靠 IP 地址来定位主机的，因此，需要在主机的名字和 IP 地址之间建立一种映射或转换机制，提供这种机制的系统称为域名系统。

域名系统（Domain Name System，DNS）给出了网上主机域名命名规则，以及对应 IP 地址的查询和翻译等。DNS 提供的应用服务称为域名服务。

域名系统将整个互联网按树形的层次结构进行划分，每一个划分称为“域”，最高层对应树的根结点，为顶级域，并为每个顶级域规定了通用的顶级域名，如 cn 是中国的顶级域名。网络信息中心将顶级域的管理权授予指定的管理机构，各个管理机构再为它们所管理的域分配二级域名，并将二级域名的管理授予其下属的管理机构，这些管理机构再分配三级域名，……，如此层层细分，就形成了互联网树形层次结构的域名结构，如图 1-20 所示。

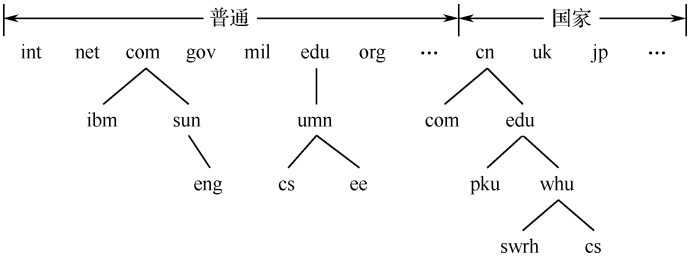


图 1-20　互联网树形层次结构的域名结构

在域名系统中，每个域都是由不同的组织来管理的，而这些组织又可将其子域分给其他的组织来管理。这种层次结构的分布式管理的优点是：各个组织在它的内部可以自由选择域名，

只要保证组织内的唯一性即可，而不用担心与其他组织内的域名冲突。

由于互联网用户发送和接收数据必须使用 IP 地址进行路由选择，因此用户主机域名首先应转换为 IP 地址，这种转换过程称为域名解析。域名解析包括正向解析（域名到 IP 地址）和反向解析（IP 地址到域名）。域名解析是由一系列服务器完成的，这些实现域名解析的服务器称为域名服务器。终端用户与域名服务器之间、各域名服务器之间都采用 C/S 模式。

通过某一后缀的域名服务器一定能够找到所有具有这个后缀的域名到其 IP 地址的映射。具体过程是由用户入网处的域名服务器按照域名从右向左的顺序进行查询处理。

① 如用户主机设置的域名服务器的地址数据库中含有对应的域名地址，则立即转换。

② 如用户主机设置的域名服务器管辖网区中最近有用户查询过同一域名，并被正确解析，由于该域名服务器将在缓存区中保留有关记录一段时间，也可立即转换。

③ 如在用户主机设置的域名服务器中查不到该域名，则先向最高一级（国家名码）域名服务器查询，然后向下逐级向相应的域名服务器查询，直到将整个域名转换为 IP 地址号为止。

1.3.4 网络协议工作过程

除了信号级的传输信道外，网络数据传输的机理在于网络中的服务器设备、席位终端、网络互联设备对 TCP/IP 协议的实现。计算机网络中的数据并不是在两个对等实体间直接传送的，而是由发送方实体将数据逐次层层传递给它的下一层，直至最下层，通过物理介质实现实际通信；数据到达接收方后，由接收方最下层逐次层层向上传递直至接收实体，完成对等实体间的通信。也就是说，除了在物理介质上进行的是实际通信之外，其余各对等实体间进行的都是虚拟通信。主机终端和网络设备利用 TCP/IP 实现数据传输的逻辑流程，如图 1-21 所示，从中可见，路由器作为网络互连设备在转发分组时最高只用到了网络层。

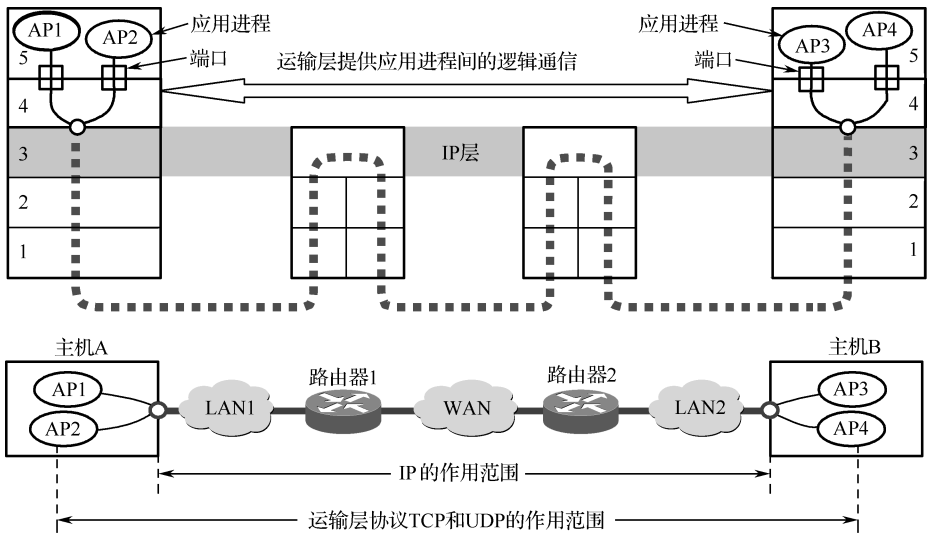


图 1-21 网络进程间的逻辑通信流程

在计算机网络中，数据都是从源端发出经过网络传达到目的端。图 1-22 示例了主机 A 中的通信进程 PA 与主机 B 中的通信进程 PB 进行数据传输的工作过程。在发送方数据由上层向下层递交的每一个过程中都有一个“打包”的过程；同样在接收方，随着向上层的递交，每一

层都有一个“解包”的过程。

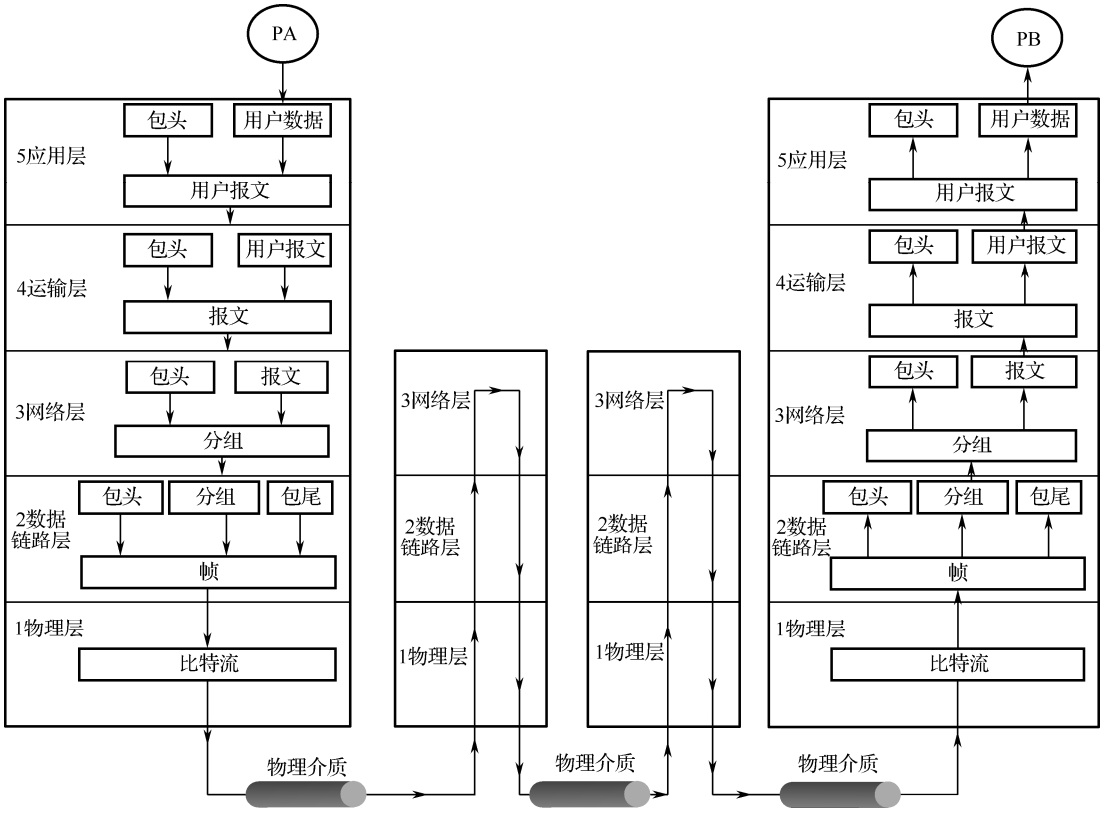


图 1-22　网络中数据流动过程

这个过程与邮政系统处理信件的处理过程十分相似。如当收信人所在地的邮政局收到邮包后，一定需要打开邮包，这是一次解包过程，得到单独的信件。当收信人收到信件后，收信人会拆开信封，这又是一次解包的过程。接收方某一层收到的数据一定是发送方对应层发送的。例如，接收方邮政局收到的邮包一定是发送方邮政局发出的。在计算机网络中也是一样，接收端收到的数据一定是发送端发出的。

在图 1-22 中，发送端的应用进程 PA 将用户数据先送到应用层，应用层上加上若干比特的 HTTP 等应用协议控制信息（称为包头），构成第 5 层的协议数据单元（称为用户报文），传到运输层；运输层收到用户报文后，再加上本层的协议控制信息（UDP 或 TCP），构成第 4 层的协议数据单元（称为报文），再交给网络层；网络层再加上本层的 IP 协议控制信息，构成第 3 层的协议数据单元（称为分组），再交给数据链路层；数据链路层分别在分组的首部和尾部加上以太网协议等控制信息，构成第 2 层的协议数据单元（称为帧），再传到物理层；物理层将帧以比特流的方式传送到物理传输介质（如双绞线电缆）上。

比特流经网络物理介质到达第一个相邻节点后，从该节点的物理层上升到数据链路层，数据链路层根据以太网协议等控制信息进行必要的操作后，剥去控制信息，将剩下的协议数据单元上交网络层；网络层根据 IP 协议控制信息进行必要操作完成路由选择后，更新网络层控制信息，又下传到数据链路层；数据链路层再加上控制信息送到物理层。最后，通过网络的物理介质传送到接收端。在接收端从第 1 层上升到第 5 层，同样每一层都根据控制信息进行必要的

操作，再将控制信息剥去，把剩下的协议数据单元上交更高的一层。由此可以说，在计算机网络中传送数据的过程就是发送方层层打包的过程和接收方层层解包的过程。

下面以通过 HTTP 访问 WWW 网站服务为例，进一步说明数据包的封装与解包过程。如图 1-23 所示，首先，IE 浏览器等应用程序在用户数据的前面加上 HTTP 首部，组成一个数据包后准备通过操作系统中的 TCP 栈发送到目标网站，当数据包到达传输层时，TCP 需要为数据包加上源端口和目标端口、数据包序号和应答字段等内容，以便实现连接应答与出错重传等 TCP 中的各种特征，这些数据当作 TCP 首部被加在原来数据包的前面，由此形成一个新的数据包后再交给网络层的 IP，这个被封装后的数据包就称为 TCP 报文段。

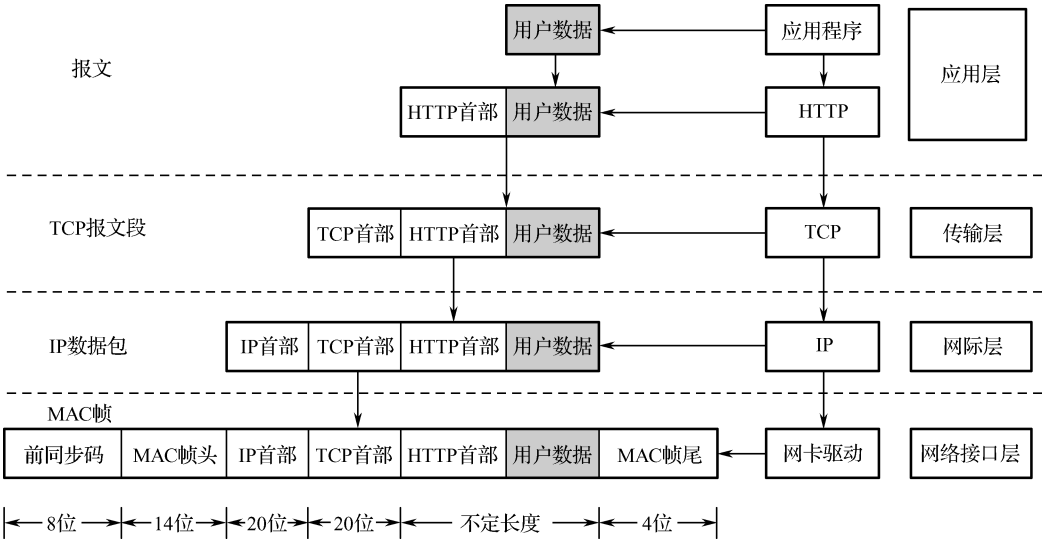


图 1-23　数据包的封装

IP 负责寻址，它需要为 TCP 段加上目标 IP 地址和自己的 IP 地址，为了让目标主机的网络层在处理数据包后能知道往传输层的哪个协议中传送，还需要标出数据包是由传输层的 TCP 协议进行传输的。现在 IP 数据包到了网络接口层的网卡驱动程序中，在这里驱动程序根据目标 IP 地址查出目标设备的 MAC 地址，在数据包的头部加上源 MAC 地址和目标 MAC 地址，同时为数据包加上一个尾部，所有这些数据形成一个数据帧（Frame）后被发送到双绞线等网络介质上。

当数据帧到达目标主机后，网络接口层将以太网首部和尾部数据去除，以恢复成 IP 数据报；IP 分析 IP 首部数据，并根据 IP 首部中的传输层协议类型将恢复的 TCP 报文段交到上层的 TCP 中；TCP 再根据 TCP 首部中的数据判断数据包的序号，检测有无丢包，并根据情况决定是否要求发送方重传，纠错后将正确的数据交到应用层的应用程序中。这时的数据包中包含 HTTP 首部和用户数据，应用程序最后处理 HTTP 首部并得到正确的原始数据。

习题

1．简述军事网络的主要作用。

2．比较广域网与局域网的差别。

3．简述 C/S 数据传输模式的优缺点。
4．计算机网络为什么要采用分组交换方式？
5．分组交换有哪些特点？
6．网络协议的三个要素是什么？各有什么含义？
7．TCP/IP 模型中各层的主要功能是什么？
8．TCP 建立连接时为什么要三次握手？
9．如何安装一台 DHCP 服务器？
10．简述 TCP/IP 的工作过程。

Chapter 2

第2章

军事网络通信基础

【主要内容】 介绍网络通信有关概念、信道复用技术和网络性能指标，包括各种传输方式的基本含义，各种编码和调制技术的基本原理，以及频分复用、时分复用、波分复用和码分复用等信道复用技术的原理与特点。

2.1 数据通信基本概念

从端到端的远程数据传输角度看，军事网络依托数据通信系统实现网络通信。数据通信系统是通过数据电路将分布在远地的数据终端设备与计算机系统连接起来，实现数据传输、交换、存储和处理的系统。数据通信系统模型如图 2-1 所示。

网络通信涉及信号、数据、信息、信道等术语。信息是指包含在消息中对人们有意义的那部分内容，而消息是指能向人们表达客观物质运动和主观思维活动的文字、符号、数据、语音和图像等，不同接收者从同样的消息量中获得的信息量是不同的，消息事件的不确定程度体现了信息量的大小。数据是把消息事件的某些属性规范化后的表现形式，是指用来描述客观事物的数字、字母和符号，以及所有输入到计算机中并被程序加工处理的符号集合。数据是装载信息的实体，信息则是数据的内在含义或解释，信息可以通过解释或使用数据来产生。信号是数据的物理表示形式，是信息的载体。

通信系统中通常使用的是电信号，即随时间变化的电压或电流信号。在网络系统中，通过传输介质传输的数据都称为信号。信号的类型与传输介质和网络设备等因素有关，如适用于电缆、光缆、微波线路等不同传输介质的电信号、光信号、微波信号等，其中电信号可以

分为模拟信号和数字信号两种形式。信道是传送信号的一条通路，由传输介质及相应的附属设备组成。同一个传输介质上可以同时存在多条信号通路，即一条传输线路上可以有多个信道。例如一条光缆可以供上千对人同时通话，它就有上千个电话信道。通信设备可分为模拟通信设备和数字通信设备，从而使传输信道分为模拟传输信道和数字传输信道。

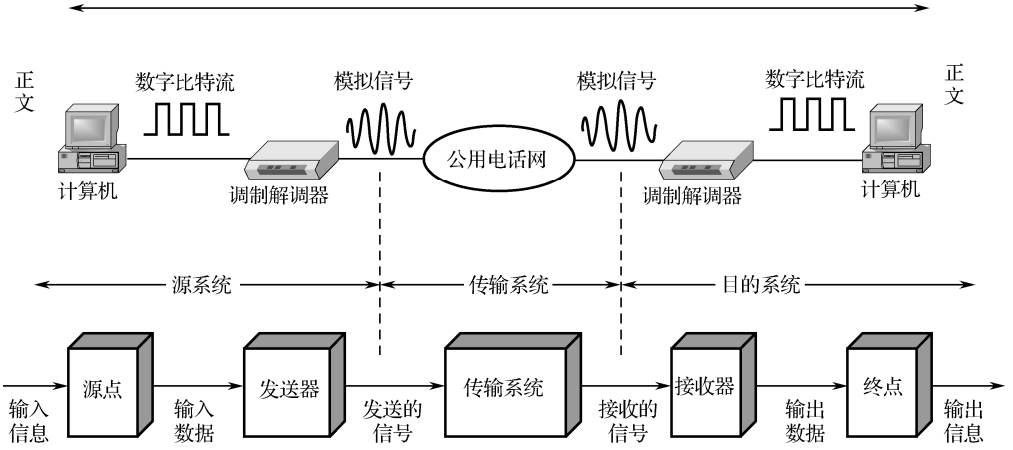


图 2-1　数据通信系统模型

2.1.1　通信传输方式

1．基带传输和频带传输

根据数据传输系统在传输由终端形成的数据信号的过程中是否搬移数据信号的频谱，即是否进行调制，可把传输方式分为基带传输和频带传输两种。

基带传输是一种不搬移数据信号频谱的传输方式。基带传输的最简单例子是由电话拨号盘向交换机传送的直流断续拨号。因基带信号所包含的频率成分范围极宽（一般从直流至高频），所以只限在能通过此频率分量的市内线路上使用。一般长途载波电路是通频范围仅为 300～3000Hz 的频率传输信道，故不能用于基带传输。

频带传输则是一种利用调制解调器搬移数据信号频谱的传输体制。搬移频谱的目的是适应传输信道的频率特性。

2．串行传输和并行传输

若按传输数据的时空顺序分类，数据通信的传输方式可分为串行传输和并行传输两种。数据在一个信道上按位依次传输的方式称为串行传输；数据在多个信道上同时传输的方式则称为并行传输。图 2-2（a）表示串行传输的基本原理，图 2-2（b）表示并行传输的基本原理。

串行传输有以下特点。

（1）所需要的线路数少，线路利用率高，投资小。因而，目前大多数数据传输系统（特别是长距离传输系统）都采用这种方式。

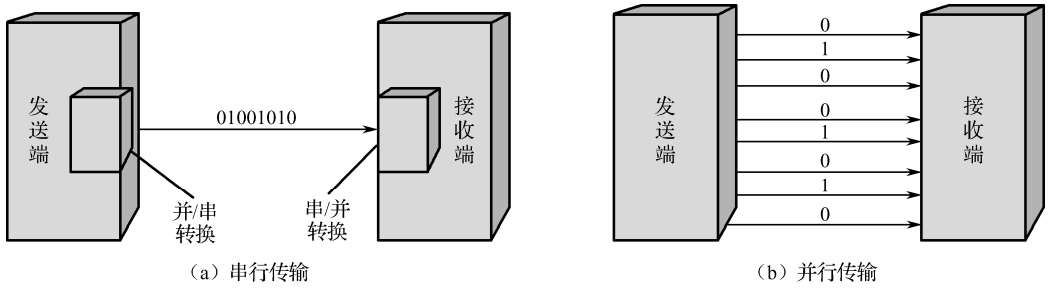


图 2-2　串行传输和并行传输的基本原理

（2）由于终端装置的输入代码形式一般是以字符为单位的并行式结构，因此在发送端和接收端需要分别进行并/串转换和串/并转换。

（3）收发之间必须实施同步措施，使其协调一致地准确工作，以确保不产生错字。

并行传输有以下特点。

（1）在终端装置和线路之间不需要对传输代码进行时序变换，因而能简化终端装置的结构；

（2）需要 *n* 条信道的传输设备，故其成本较高，因而并行传输通常用于要求传输速率高的近距离数据传输中。

3．异步传输和同步传输

在串行传输时，每一个字符是按位串行地传送的，为使接收端能准确地接收所传输的信息，接收端必须知道以下几点。

（1）每一位的时间宽度，即传输的比特率。

（2）每一个字符或字节的起始和结束。

（3）每一个完整的信息块（或帧）的起始和结束。

上述三个要求分别称为比特（位或时钟）同步、字符同步及块（或帧）同步。

通常用异步传输和同步传输两种方法来实现同步。这两种方法的区别在于对于异步传输，发送器和接收器的时钟是不同步的；而对于同步传输，两者的时钟是同步的。

在异步传输时，每一个传送的字符都有一个附加的起始位和一个或多个停止位，如图 2-3 所示。起始位与停止位的极性不同。因此在每一个连续的字符间，不管被传送的字符中的比特序列如何，至少总要有一次“1→0→1”的变换。因此，在一段空闲时间后的第一个“1→0”的变换被接收器判定为一个新字符的开始。利用一个频率为传输比特率 *n* 倍的时钟，在每一个比特周期的中心对接收的信号采样，接收设备以此来确定传送字符中每一比特的状态。

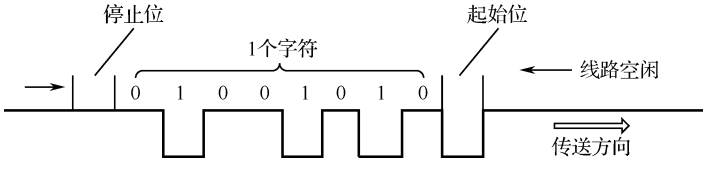


图 2-3　异步传输

由于异步传输对每个字符都使用起始位和停止位，因此在需要传送大量数据块的场合就显得太浪费了，此时可使用同步传输。同步传输是把每个完整的数据块（帧）作为整体来传输的。为使接收设备能够准确地接收数据块的信息，需要满足以下条件。

（1）接收器和发送器之间的比特（位或时钟）同步，可以通过设法把发送端的时钟信息载

入传送的比特流中，然后由接收器提取的办法来实现。

（2）为确保接收器按正确的字节边界可靠地接收比特流，所有帧由一个或多个保留字作为前导，如图 2-4 所示。

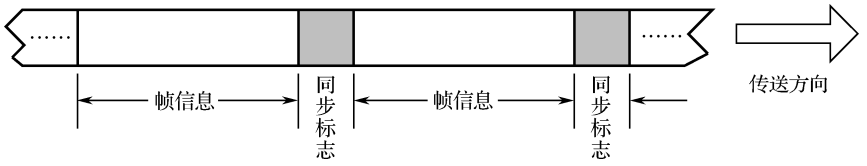


图 2-4　同步传输

（3）每一帧内容都有帧起始符和帧结束符。对于内容为字符的帧，起始符（STX）和结束符（ETX）都是保留字，它不会出现在帧中间；对于内容不是字符而是比特流的帧来说，要使用其他办法来标识帧的起始与结束，以避免在帧中出现 ETX 字符时误认为帧结束。

4．单工传输、半双工传输和全双工传输

按照数据信号在信道上的传送方向与时间的关系，传输方式可分为单工传输、半双工传输和全双工传输。

（1）单工传输是两个数据站之间只能沿一个指定的方向传送数据信号，如图 2-5（a）所示。

（2）半双工传输是两个数据站之间可以在两个方向上传送数据信号，但不能同时进行，如图 2-5（b）所示。即同一时刻只能沿一个方向传送数据信号，因此这种传输模式也称为“双向交替”模式。这种传输方式特别适用于会话式通信的场合。

（3）全双工传输是两个数据站之间可以在两个方向上同时传送数据信号，如图 2-5（c）所示。这种传输模式也称为“双向同时”模式，它与半双工传输相比要有效得多，特别适用于高速数据通信的场合。

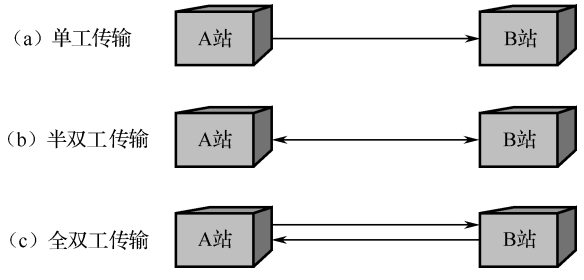


图 2-5　单工传输、半双工传输和全双工传输

上述定义中并未涉及信道上所用信号线的数目问题。通常采用四线线路实现全双工传输；二线线路实现单工传输或半双工传输。采用频分或时分复用技术及回波抵消技术时，二线线路也可以实现全双工传输。

2.1.2　数据调制与编码

原始的数据信号不仅包含直流分量在内的低频率分量，还含有许多其他频率成分的谐波分量，必须经过编码或调制才能在传输介质上传输。例如，打电话是将模拟信号（声音）调制为另一种模拟信号。将模拟数据调制为另一种模拟信号进行传输，既简单又经济。这种使用调制

技术把频带信号的带宽搬移到其他频谱部分，使各个信号在频谱中的位置不同，多个信号就可以共用同一传输介质，即频分多路复用技术。编码器将模拟数据编码为数字信号；MODEM 将数字信号调制为模拟信号；数字发送器将数字信号编码为另一种数字信号。选择某种编码技术的目的可能是因为节省带宽，便于同步，或者是为了减少差错率，也可能是由于受到传输介质本身特性的限制。

一般说来，数字数据或信号编码为另一种数字信号，其编码设备比数字到模拟的调制设备更简单、更廉价。模拟数据编码为数字信号后，就可以使用先进的数字传输和交换设备。数字数据转换为模拟信号，是为了利用适于传播模拟信号的传输介质。

1．数字信号的模拟调制

数据通信是从传统的公用服务电话网（Public Service Telephone Network，PSTN）开始的，PSTN 人为地把传输的信号限制在人类语音的频率范围内（300～3400kHz），以降低每个话路所需的带宽。然而计算机内的信息是由二进制脉冲“0”和“1”组成的数字信号，而在电话线上传递的只能是模拟电信号。因而，数字设备必须通过调制解调器与网络相连，将数字信号转换成模拟信号，或将模拟信号转换成数字信号。

数字信号转换为模拟信号的基本调制技术比较简单，有调幅、调频、调相三种，如图 2-6 所示。

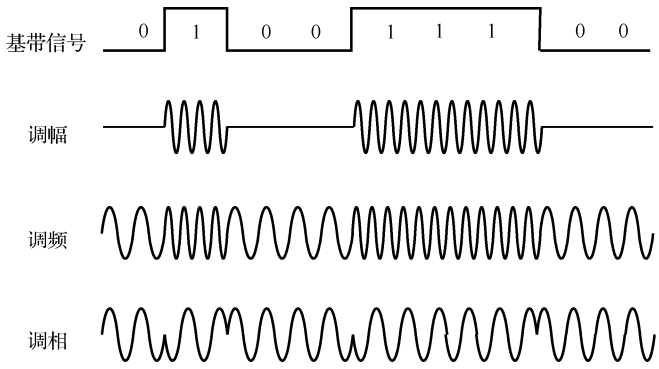


图 2-6　三种数字调制技术

2．模拟信号的数字编码

把模拟数据转变成数字数据，称为数字化编码。模拟数据转化为数字数据的目的是利用数字信道来传输模拟数据，如语音是模拟数据，为了避免由于模拟传输带来的噪声，充分利用数字传输的优点，要求把模拟数据转换成数字数据。信号的数字化由编/解码器（codec）完成。这里主要介绍脉码调制（Pulse Code Modulation，PCM）技术。

PCM 脉码调制以采样原理为基础，之后进行量化和编码。

（1）采样

按照奈奎斯特采样定律，如果一个信号 $f(t)$以固定的时间间隔并以高于信号最大主频率两倍的速率进行采样，那么这些样本就包含了原信号中的所有信息。根据这些样本，通过使用低通滤波器，就可以重建信号 $f(t)$。例如，语音的最大带宽是 4000Hz，则采样频率为 8000Hz，语音数据的频率在 4000Hz 范围内，则每秒采集 8000 个样本就足以完全描绘出这个语音数据了。

（2）量化

在图 2-7（b）中，每个采样值都是信号的幅度值。因为在实数域内取值，所以需要将它们变为整数值。方法是将信号幅值分布的区间分成均匀的若干等级，每个采样值转换为最接近等级的整值，这个过程称为量化。量化的等级可以看作码元的状态，显然，量化的等级越多，每个码元携带的信息量就越丰富，就能更多地保留原始信号的信息。

（3）编码

如图 2-7（c）所示，量化后的整数幅值要用 *n* 位二进制数来表示，如 *n*=3 时， 5 用 101 来表示，这就是编码产生的数字信号。本例的最后编码为 101 111 110 011 100 100…。经过编码后的数字信号即可进行发送，如语音传输的频率为 4000Hz，以 8000Hz 采样，用 7 位二进制数编码，则其数据传输率为 8000×7=56Kbps。若用 8 位编码，则其数据传输率为 8000×8=64Kbps。

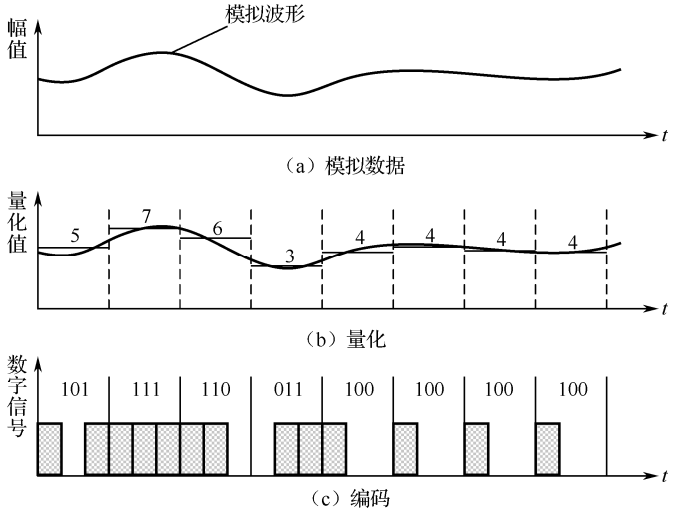


图 2-7　脉冲编码调制过程

在接收端，执行相反的过程，再生成模拟数据。注意：通过量化，原始信号仅为近似值，而不能精确恢复，这个影响称为量化误差。编码的位数越多则量化误差越小。

目前，国际上存在着两个利用 PCM 的标准，一个是美国的 24 路 PCM，称为 T1 标准，其链路速率为 1.544Mbps；另一个是欧洲的 30 路 PCM，称为 E1 标准，其链路速率为 2.048Mbps，我国采用 E1 标准。正是由于 T1 和 E1 的存在，在 20 世纪 70 年代以前，国际间的语音和数据通信缺乏统一的传输速率标准，使得互连难以实现。后来 ITU 制定了同步光纤网络 SONET/SDH 标准，才解决了这个问题。

3．数字数据编码

在数据通信设备内部，由于各电路功能模块之间及模块内部的元器件之间距离很短，且工作环境可以通过各种措施加以保护，所以通常将原始的二进制并行或串行数据直接进行传输。而在远程传输数据时，为了便于同步，减少在信号传输介质中的传输损耗并提高抗环境干扰能力，需要对传输的数据进行编码。

ITU-T 建议使用的基带传输码型有 20 余种，常用的有以下几种。

（1）双相码

双相码又称分相码或曼彻斯特（Manchester）码。它的编码规则是：在每位信号的中间有一个跃变，对于数据“1”，用前半周期为 0 电平、后半周期为+E（或−E）电平；对于数据“0”则用前半周期为+E（或−E）电平、后半周期为 0 电平，即通过传输每位数据中间的跳变方向表示传输数据的值，波形如图 2-8（a）所示。这种编码方式具有下述优点：首先每传输一位数据都对应一次跳变，有利于同步信号的提取；其次，对于每一位数据，其+E（或−E）电平和 0 电平占用时间相同，不存在直流分量，有利于判决电路工作。其缺点是数据编码后脉冲频率为数据传输速度的 2 倍。这种编码被广泛地用于 10M 位以太网（Ethernet）和无线寻呼的编码中。

（2）差分双相码

它是曼彻斯特码的改进。其编码利用了差分编码技术，每位中间都跃变，但区间开始时遇 1 不变遇 0 跃变，如图 2-8（b）所示。它与曼彻斯特码具有同样的特性，获得了广泛的应用。

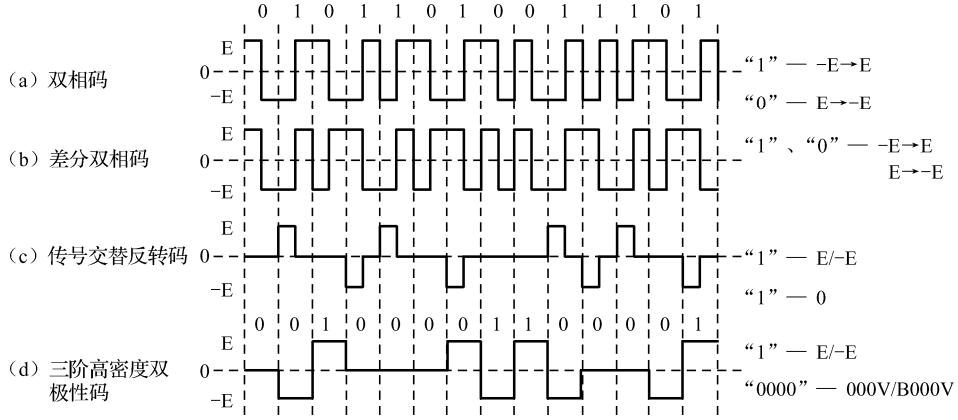


图 2-8　常用的传输码型

（3）传号交替反转码

传号交替反转码记作 AMI 码。对于数据代码中的“1”，顺序交替地用+E 和−E 电平表示，对于数据代码中的“0”，仍变换为传输码的 0 电平，如图 2-8（c）所示。这种编码具有下述特点：首先容易出现连“0”串，不利于提取同步定时信号；其次是无直流分量，有利于在不允许直流和低频信号通过的介质和信道中传输，有利于判决电路工作；第三，其数据代码“1”对应的传输码的电平正负交替，有利于误码观察。它是脉码调制编码中较常用的一种码型。

（4）三阶高密度双极性码 HDB3

HDB3 编码方法建立在 AMI 码的基础上，即先把数据代码变换成 AMI 码，再对 AMI 码进行变换。HDB3 码除了有 AMI 码的优点外，还克服了其缺点，ITU-T 建议将其作为 PCM 的传输码型之一。

2.1.3　军事通信协议

TCP/IP 被用于因特网，也广泛用于各种军事信息系统网络。从数据传输的角度看，军事

网络技术的核心和基础在于 TCP/IP。军事网络系统的互连可以依靠光纤宽带网、电话交换网、卫星通信网及民用通信设施，这些设施都是基于 IP 实现网络互连互通的。

军事信息系统基于 IP 实现网络互连主要有两种方式。一种互连方式是系统通过路由器由光纤、无线通信设备接入网络或其他系统，通过 TCP/IP 网络协议实现互连，支持高速互连，满足大容量的信息传输；另一种互连方式是拨号入网方式，它通过电话线接入网络，同样实现基于 IP 的网络连接，一般只支持低速传输，可用于快速机动、演习及不具备宽带通信条件的场合。

1．军事信息传输对网络协议的需求

单纯地从网络互连和资源共享的角度看，网络技术的关键就是各种网络协议。军事信息传输具有实时性强、可靠性高、抗干扰能力强等要求，这些要求需要通过协议规范才能实现。

（1）实时性强

军事信息系统要求信息传输速度要快，尽量减少中转环节，最好采用专用信道。若采用公共数据交换网，也要保证高优先等级，以保证军事信息的时效性。

（2）可靠性高

军事信息系统无论是在战时还是平时，始终处于高度戒备状态，军事信息的传递不能有瞬间的中断。因此，信息传输系统要能可靠地连续工作。一方面要求数据传输设备要可靠，有冗余措施，另一方面要求有备份通信手段。

（3）抗干扰能力强

整个数据传输系统对复杂的电磁环境要有较好的适应性，具有较强的抗干扰能力、多种加密手段和抗毁措施。

网络协议是计算机网络中进行数据交换而建立的规则、标准或约定的集合。军事信息传输选用计算机网络 TCP/IP 协议作为统一的网络传输协议，主要原因在于：IP 可横跨局域网、广域网，几乎所有局域网、广域网系统及设备均支持 IP，IP 是不同媒体传输方式的最佳协议，其传输响应时间较好、协议交互少，较适合数据高速传输的需要。TCP 作为 IP 的上层协议，是支持端节点之间通信的传输层协议，可提供面向连接的流式通信形态的应用程序，具有修正错误、顺序控制、流控制、阻塞控制等功能，为各应用程序之间提供可靠的通信。

2．军事网络的协议层次

军事网络互连依靠的通信资源主要有军用电话交换网、军用数据交换网、卫星通信网及民用通信设施。从使用的通信协议看，军事广域网主要采用 POS 技术，以 IP/PPP/SDH+MPLS 技术组网；军事局域网主要采用以太网技术，以 IP/Ethernet/FIBER 或 WDM+MPLS 技术组网。

TCP/IP 是计算机网络的基础性协议，也是军事信息传输的基础性协议。无论是地面信息系统，还是空中信息网或天基信息网，都可以基于 IP 提供通信节点之间的高速军事信息传输能力，实现信息网络的互连互通，实现不同军事信息系统之间连续可靠的信息传输。

多数军事信息系统网络的协议层次结构，如表 2-1 所示。

表 2-1 军事信息系统网络的协议层次结构

<table>
<tr><td rowspan="2">物理层</td><td colspan="2">数据链路层</td><td rowspan="2">网络层</td><td rowspan="2">传输层</td><td colspan="3" rowspan="2">应用层</td></tr>
<tr><td>MAC 子层</td><td>LLC 子层</td></tr>
<tr><td rowspan="3">宽带数据链波形</td><td>PPP</td><td rowspan="3">宽带数据链链路层协议</td><td rowspan="3">Ad Hoc 动态路由、IPv6</td><td rowspan="3">UDP、改进的 TCP</td><td rowspan="3">Qos 机制、优先级排队</td><td rowspan="3">XML</td><td rowspan="3">语音、数据、图像、视频</td></tr>
<tr><td>TDMA
DTDMA
STDMA</td></tr>
<tr><td>广播</td></tr>
<tr><td>地面网</td><td>MAC 协议</td><td>LLC 协议</td><td>IPv4、IPv6</td><td>UDP、TCP</td></tr>
<tr><td>综合数据链</td><td>PPP、MAC 协议</td><td>卫星信道等链路层协议</td><td>IPv4/IPv6</td><td>UDP</td><td colspan="3">消息格式及处理规则</td></tr>
<tr><td colspan="7">安全、保密</td></tr>
</table>

（1）应用层

该层协议提供面向用户的各种业务应用，如信息报文传输格式协议等，包括具有 QoS 要求的实时语音、数据和图像业务，支持各种类型格式。应用层可以对业务进行分类，在同一类业务中还可以进行优先级划分，为不同的信息提供不同的 QoS 保障。

（2）传输层

该层协议为应用层提供可靠的端到端服务，并根据网络层的特性来高效利用网络资源，特别是要考虑对由于无线信道的固有缺陷及网络节点移动造成的分组丢失或延迟的补偿。主要涉及 TCP 和 UDP 两类传输协议。

（3）网络层

该层协议包括组网协议与路由协议，实现邻居发现、分组路由、访问控制、拥塞控制等功能，根据不同的业务选择最佳的数据传输路径，达到系统性能的最优化，并通过各链路内及不同链路间的互连，形成一个更广范围的互连互通网络。该层主要涉及 IP 协议。

（4）数据链路层

该层协议中的物理访问控制（MAC）子层控制网内节点对共享信道的访问，响应应用层的业务分类和优先级划分，保证最高优先级的消息首先接入网络，相同的优先级随机选择时隙，支持的信道接入协议包括基于信道划分的 TDMA、STDMA、轮询机制、点对点等。逻辑链路控制（LLC）子层负责数据流的复用、数据帧的检测、分组的确认、优先级排队、差错控制和流量控制等。

（5）物理层

该层协议规范信号在信道的通信过程，实现信号的检测、调制解调、信道加密解密、信号发送和接收等，包括语音通信波形、各类数据链信道波形、其他数据通信波形等波形信号的传播规则。

（6）安全与保密

该类协议贯穿协议栈的各个层次中，保证各层协议运行的安全性。安全功能要求包括物理安全、设备安全、信道安全、多域互连安全、业务安全、用户安全、管理安全、安全审计。保密体制主要包括密码加密算法、信号签名的加密方法、密钥管理算法等。

2.2 信道多路复用技术

在通信系统中，信道所提供的带宽往往比所传送的信号的带宽宽得多，此时如果一条信道只传送一路信号就过于浪费。信道复用指的是将多路独立信号在一条信道上传输。因此，信道复用的条件是信道的传输能力大于各路信号的平均传输需求（往往如此）。信道复用的目的是充分利用信道的容量，尽可能不重复建设通信线路，提高信道传输效率。

信道复用的基本原理是把一个物理信道按一定的机制划分为多个互不干扰、互不影响的逻辑信道，每个逻辑信道各自为一个通信过程服务，每个逻辑信道均占用物理信道的一部分通信容量。信道复用技术是使多路无关信号共享一个物理信道传输，到达接收端后再进行分离的技术，如图 2-9 所示。

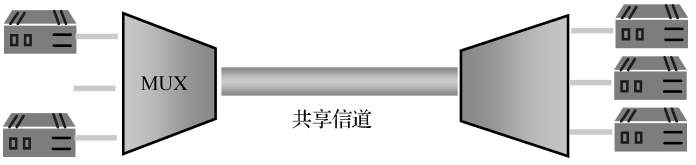


图 2-9　信道复用示意图

实现信道复用的核心设备是多路复用器（Multiplexer）和多路解复用（分配）器（Demultiplexer）。前者在发送端根据某种约定的规则把多个低速（低带宽）的信号合成一个高速（高带宽）的信号，后者在接收端根据同一规则把高速信号分解成多个低速信号。

为了区分一条信道上的多个用户的信号，理论上可以采用正交划分的方法。也就是说，凡是在理论上正交的多个信号，在同一条信道上传输到接收端后都可以利用其正交性完全区分开。在实际中，常用的正交划分体制主要有频分制、时分制、波分制和利用正交编码划分的码分制，对应技术主要有频分复用（Frequency Division Multiplexing，FDM）、时分复用（Time Division Multiplexing，TDM）、波分复用（Wavelength Division Multiplexing，WDM）和码分复用（Code Division Multiplexing，CDM）。

2.2.1 频分复用技术

频分复用技术是将传输信道的频率带宽分成互不重叠的多个子频带，每个子频带作为一个逻辑信道传输一路数据信号。频分复用技术多适用于广播、电话、有线电视等模拟信号。

为避免相邻子频带之间的相互串扰影响，一般在两个相邻的子频带之间留出一部分空白频带（保护频带）。每个子频带的中心频率用作载波频率，使用一定的调制技术把需要传输的信号调制到指定的子频带载波中，再把所有调制过的信号合成在一起传输。接收端各路信号的区分：依赖于载波中心频率。

图 2-10 示出了频分多路复用原理图。语音信号频分多路载波通信系统是其典型用例。

FDM 的特点：第一，一个信道在同一时刻能同时传送多路信号，每路信号在同样的时间占用不同的频带；第二，要求物理信道的可用频带超过各路信号所需带宽和；第三，利用各路信号在频率域不相互重叠来区分，若相邻信号之间相互干扰，将会使输出信号产生失真；第四，

为了防止相邻信号之间的相互干扰，应合理选择载波频率 f_1，f_2，…，f_n，并使各路已调信号频谱之间留有一定的保护带。

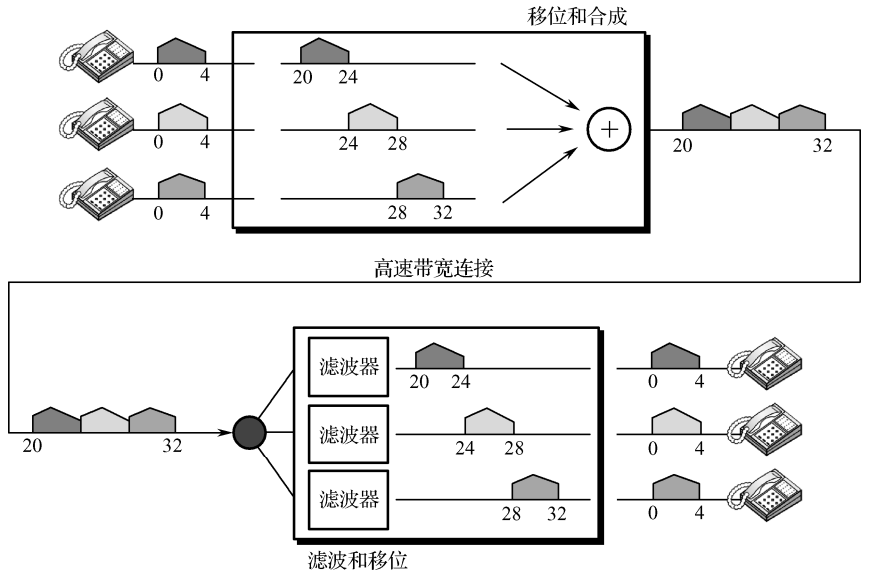


图 2-10　频分复用原理图

FDM 的主要优点：实现相对简单，技术成熟，能较充分地利用信道频带，系统效率较高。但是它的缺点也很明显：保护频带的存在大大地降低了 FDM 技术的效率；信道的非线性失真改变了它的实际频带特性，易造成串音和互调噪声干扰；所需设备量随输入路数的增加而增多，且不易小型化；频分多路复用本身不提供差错控制技术，不便于性能监测。因此，在实际应用中，FDM 正在被时分多路复用所替代。

2.2.2　时分复用技术

时分复用技术将物理信道按时间分成若干时间片轮换地分配给多路信号使用，每一路信号在自己的时间片内独占信道传输。时分复用技术多用来传输计算机网络、移动通信等中的数字信号，也可分时传输模拟信号。

TDM 的原理：由于基带传输系统采用串行传输的方法传输数字信号，因此不能在带宽上划分。TDM 技术在信道使用时间上进行划分，按一定原则把信道连续使用时间划分为一段段很短的、等长的时分复用帧，把各个时间帧分配给不同的通信过程使用。由于时间帧的划分一般较短暂，可以想象成把整个物理信道划分成多个逻辑信道，交给各个不同的通信过程来使用，每一个时分复用的用户在每一个帧中占用固定序号的时隙。每一个用户所占用的时隙周期性地出现，其周期就是 TDM 帧的长度。只要发送端和接收端的时分多路复用器能够按时间分配同步地切换所连接的设备，就能保证各路设备共用一条信道进行通信，而且相互之间没有任何影响，相邻时间帧之间没有重叠，信道利用率更高。

图 2-11 示出了时分复用原理图，3 路通信设备连接到一条公用信道上，发送端时分复用器按照一定的次序轮流地给各个设备分配一段使用公用信道的时间，即时隙。当轮到某个设备使用信道传输信号时，该设备就与公用信道逻辑上连接起来，而其他所有设备与信道的逻

辑联系被暂时切断，待指定的通信设备占用信道的时间一到，时分多路复用器就将信道切换给下一个被指定的设备。依次类推，一直轮流到最后一个设备，即一个 TDM 帧，然后又重新开始。

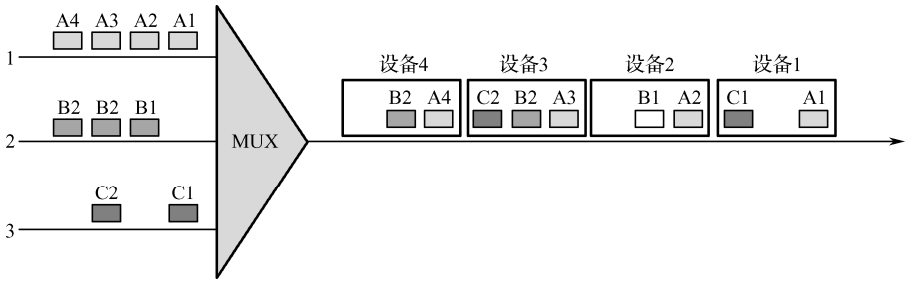


图 2-11　时分复用原理图

TDM 的工作特点是：第一，将信道的传输时间划分成若干时隙，并将各时隙轮流地分配给各路信号，使多路信号分时地在同一个信道内传输，时间域上互不重叠；第二，任一瞬间只有一路信号占用线路，但每路信号都占用整个信道频带；第三，就一段时间而言，公用信道上传送着按时间分隔的多路复合信号；第四，只要时分多路复用器的扫描操作适当、采取必要的缓冲措施、合理地分配时隙，就能够保证多路通信的正常进行。

TDM 的缺点：在高速通信中效率较低。当某用户无数据发送时，其他用户也不能占用该通道，会造成带宽浪费。改进：用户不固定占用某个时隙，而是动态地按需分配时隙。此时复用器传输的数据只来自正在工作的设备。以这种动态分配时隙方式工作的 TDM 称为统计时分多路复用（Static TDM，STDM）。STDM 帧的长度是不固定的，同时时隙的位置也失去了意义。因为事先并不知道哪个数据源产生的数据会占用哪个位置的时隙。为了使接收端的复用器能正确分离各路数据，必须使每一时隙中带有地址信息或数据源编号信息。所以，STDM 的每个时隙都存在额外开销，因为每个时隙中既包含数据又包含地址或信源编号。

2.2.3　波分复用技术

波分复用技术（WDM）是将各信道的信号调制成不同波长的光，各路光波经过一个棱镜（或衍射光栅）合成一个光束在光纤干道上传输。波分多路复用是光纤信道中光信号的频分复用。

WDM 的原理：在光纤通信中，为了实现长距离范围的高速传输，通常采用波分复用技术和光纤放大器。采用波长分割技术实现多路复用，实现时采用光学（如衍射光栅）系统的衍射光栅原理将不同信道的信号调制成不同波长的光，并复用到光纤信道上。接收端各路信号的区分：依赖于光信号的波长（频率）。波分复用原理图如图 2-12 所示。

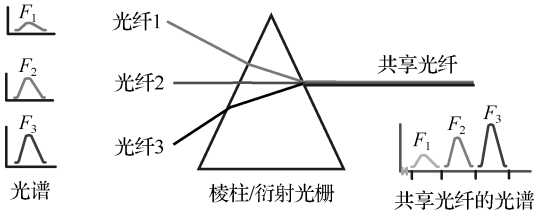


图 2-12　波分复用原理图

最初，人们只能在一根光纤上复用两路光载波信号，而后随着技术的进步，其复用的路数越来越多。目前，一条现有的普通单模光纤可传输的带宽极宽，仅 1.55μm 就可传输 10 000 个光信道，其间隔为 2.2GHz。在一根光纤上复用 80 路或更多路的光载波信号称为密集波分复用（Dense Wavelength Division Multiplexing，DWDM）。对于具有 100 根速率为 2.5Gbps 光纤的光缆，采用 16 倍的密集波分复用技术，可以实现的总数据传输速率达 4Tbps。

图 2-13 为密集波分复用原理图。图中，表示 8 路传输速率均为 2.5Gbps 的光载波（其波长均为 1310nm）。经光调制后，分别将波长变换到 1550～1557nm，每个光载波相隔 1nm（注：这里仅为了便于说明问题，实际工程上光载波的间隔一般是 0.8nm 或 1.6nm）。这 8 个光载波经过复用器后，在一根光纤上传输数据的总速率就达到 8×2.5Gbps=20Gbps。但是，由于光信号在光纤上传输会有衰减，必须对衰减了的光信号放大才能继续传输。图 2-13 中使用的光放大器为掺铒光纤放大器（Erbium Doped Fiber Amplifier，EDFA），它不需要进行光电转换而可以直接对光信号进行放大，并且在 150nm 波长附近有 35nm（即 4.2THz）频带范围提供较均匀的、最高可达 40～50dB 的增益。两个 EDFA 之间的中继距离可达 120km。这与以往的“光—电—光”转换模式相比，对于相距 600km 的两个通信站，如采用光频分复用技术，只需使用 4 个 EDFA；而采用“光—电—光”转换方案，则每隔 36km 需要加入一个再生中继器，进行光电转换、放大和电光转换，因此，总共需要 16 个再生中继器。

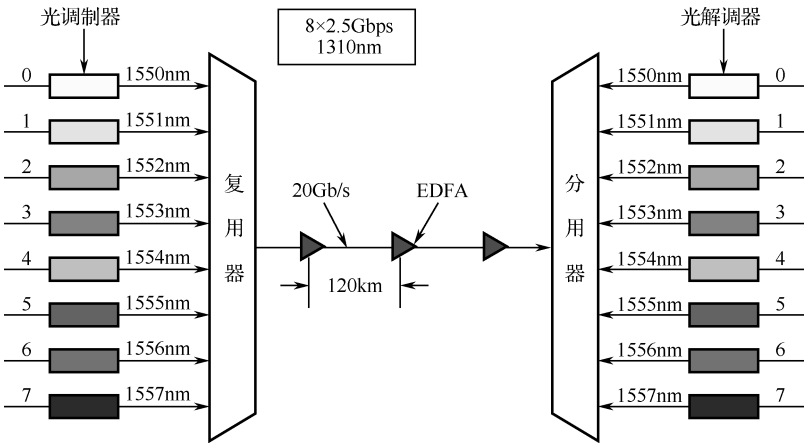


图 2-13　密集波分复用原理图

WDM 的特点：第一，将主干光纤的整个波长频带划分为若干个波长范围，各路信号各占用一个波长范围，经光复用器复用后在主干光纤中传输；第二，使用掺铒光纤放大器（EDFA）将衰减的光信号放大（不需要光电转换），从而实现远距离传输。

2.2.4　码分复用技术

码分复用是按照码型结构的差别来区分信号的。由于各用户使用了经过特殊挑选的不同码型，它们可以在同样的时间内使用同样的频带进行通信，而不会相互干扰。因此，如果从频域或时域的角度来观察，多个码分复用信号是互相重叠的。

码分复用原理：在 CDM 中，每一个比特时间被划分为 *m* 个间隔，称为码片（chip）。通常，*m* 的值是 64 或 128。使用 CDM 的每一个站被分派一个唯一的 Mb 码片序列。一个站如果要发

送比特 1，则发送它自己的 *m* bit 码片序列。如果要发送比特 0，则发送该码片序列的二进制反码。在实用的系统中，码片序列使用的是伪随机序列。

为了简单，假设 *m*=8，分派给 A 站的 8bit 码片序列是 00011011。为了方便，以后将两码片中的 0 写成−1，将 1 写为+1。因此 A 站的码片序列是（−1 −1 −1 +1 +1 −1 +1 +1）。当 A 站发送比特 1 时，它就发送序列（−1 −1 −1 +1 +1 −1 +1 +1），而当 A 站发送比特为 0 时，它就发送（+1 +1 +1−1 −1 +1 −1 −1）。

若假定 A 站发送的数据信号率为 *n*bps。由于每一个比特要变成 *m* 个比特的码片，因此 A 站实际上发送的数据率提高到 *mn* bps，同时 A 站所占用的频带宽度也提高到原来数值的 *m* 倍。其实，这属于直接序列的扩频通信方式。

CDM 复用的特点：第一，分派给每一个站的码片不仅互不相同，并且必须互相正交。令向量 *A* 表示 A 站的码片向量，再令 *B* 表示其他任何站的码片向量。两个不同站的码片序列正交，即向量 *A* 和 *B* 的内积都是 0：

$$A \cdot B = \frac{1}{m}\sum_{i=1}^{m} A_i B_i = 0$$

第二，任何一个码片向量的规格化内积都是 1，即

$$A \cdot A = \frac{1}{m}\sum_{i=1}^{m} A_i A_i = \frac{1}{m}\sum_{i=1}^{m} A_i^2 = \frac{1}{m}\sum_{i=1}^{m} (\pm 1)^2 = 1$$

如果一个码分复用通信系统中 X 站要接收 A 站发送的数据。X 站就必须知道 A 站所特有的码片序列。X 站使用它得到的码片向量 *A* 与接收到的未知信号进行求内积的运算：所有其他站的信号都被过滤掉（指其内积的相关项都是 0），而只剩下 A 站发送的信号。当 A 站发送比特 1 时，在 X 站计算内积的结果是+1，当 A 站发送比特 0 时，内积的结果是−1。

码分复用技术最初用于军事通信。现在已广泛应用于民用移动通信当中，特别是在无线局域网中。采用 CDM 可提高语音质量和数据传输可靠性，减少干扰对通信的影响，增大通信系统的容量（是 GSM 的 4～5 倍），以及减少平均发射功率等。码分复用技术允许用户在任意时刻随机接入任何信道，克服了不同用户必须根据固定安排使用信道的局限，这在局域网多路接入时极为方便。但这种简化和方便是以信道带宽的低效利用为代价的。

2.3 网络性能指标

网络常用的性能指标有速率、带宽、吞吐量、时延、时延带宽积、往返时间（RTT）、利用率等，最主要的两个性能指标就是带宽与时延。

1．速率

比特（bit）是计算机中数据量的单位，也是信息论中使用的信息量的单位。Bit 来源于 binary digit，意思是一个“二进制数字”，因此一个比特就是二进制数字中的一个 1 或 0。

速率即数据率（data rate）或比特率（bit rate），是指单位时间内所传输信号的二进制位数，是计算机网络中最重要的性能指标。速率的单位是 bps，或 Kbps、Mbps、Gbps 等。速率往往指额定速率或标称速率。

2．带宽（bandwidth）

“带宽”本来是指信号具有的频带宽度，单位是赫（或千赫、兆赫、吉赫等）。一个特定的信号是由许多不同的频率成分组成的。因此，一个信号的带宽是指该信号的各种不同频率成分所占据的频率范围。衍生含义就是线路允许通过的信号频带范围。

现在“带宽”是数字信道所能传送的“最高数据率”的同义语，即信道允许的最大数据传输速率，以信道每秒能传送的信息比特数为单位，常记为 bps，即“比特每秒”，或 bps（bit/s）。在时间轴上信号的宽度随带宽的增大而变窄。

带宽与速率的区别是，前者表示信道的最大数据传输速率，是信道传输数据能力的极限；而后者是实际数据传输速率。就像公路上的最大限速与汽车实际速度的关系一样。信道的带宽与采用的传输介质、信号的调制方法、变换器性能等密切相关。当信号带宽大于信道带宽时，信号就不能在该信道上传送，或者传送出的信号将失真。

3．吞吐量（throughput）

吞吐量表示在单位时间内通过某个网络（或信道、接口）的数据量。

吞吐量常用于对现实世界中的网络的测量，以便知道实际上到底有多少数据量能够通过网络。吞吐量受网络带宽或网络额定速率的限制。额定 100Mbps 的网络的典型吞吐量可能只有 70Mbps。

4．时延（delay 或 latency）

发送时延（传输时延）：发送数据时，数据块从节点进入传输媒体所需要的时间。也就是从数据块的第一个比特开始发送算起，到最后一个比特发送完毕所需的时间。发送时延=数据块长度/信道带宽。

传播时延：电磁波在信道中传播一定的距离而花费的时间。传播时延=信道长度/电磁波在信道上的传播速率。

处理时延：数据在交换节点为存储转发而进行必要处理所花费的时间。

排队时延：节点缓存队列中分组排队所经历的时延。排队时延的长短往往取决于网络中当时的通信量。

数据经历的总时延就是发送时延、传播时延、处理时延和排队时延之和：总时延 = 发送时延+传播时延+处理时延+排队时延。

需要指出的是，信号传输速率（即发送速率）和信号在信道上的传播速率是完全不同的概念。“在高速链路（或高带宽链路）上，比特应当跑得更快些”是不对的。对于高速网络链路，提高的仅是数据的发送速率，而不是信号在链路上的传播速率。“光纤信道的传输速率高”指的是向光纤信道发送数据的速率可以很高。光纤实际上比铜线的传播速率还慢（每秒 20.5～23.1 万公里）。

5．时延带宽积和往返时延

链路的时延带宽积又称为以比特为单位的链路长度，表示链路可容纳多少比特。时延带宽积=传播时延×带宽。

往返时延（Round-Trip Time，RTT）表示从发送端发送数据开始，到发送端收到来自接收

端的确认（接收端收到数据后立即发送确认），总共经历的时延。

6．利用率

网络利用率则是全网络的信道利用率的加权平均值。信道利用率是指某信道有百分之几的时间是被利用的（有数据通过）。完全空闲的信道的利用率是零。信道利用率并非越高越好，过高会产生非常大的时延。根据排队论的理论，当某信道的利用率增大时，该信道引起的时延也就迅速增加，如图 2-14 所示。

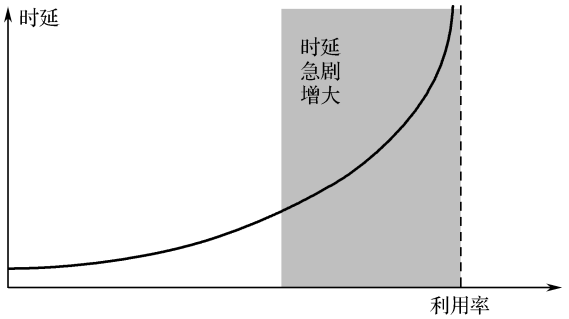


图 2-14　网络时延与利用率的关系

习题

1．数字调制技术有哪几种？简述其原理。

2．为什么要使用信道复用技术？

3．常用的信道复用技术有哪些？

4．共有 4 个站进行码分多址 CDMA 通信。4 个站的码片序列如下。

A．（−1　−1　−1　+1　+1　−1　+1　+1）　B．（−1　−1　+1　−1　+1　+1　+1　−1）

C．（−1　+1　−1　+1　+1　+1　−1　−1）　D．（−1　+1　−1　−1　−1　−1　+1　−1）

现收到码片序列为（−1　+1　−3　+1　−1　−3　+1　+1），问哪个站发送数据了？发送的是 1 还是 0？

5．计算机网络常用的性能指标有哪些？

Chapter 3

第3章

军事局域网络技术

【主要内容】 介绍以太网技术、虚拟局域网技术、网络接入技术和有线传输介质，包括以太网的协议标准、工作原理和交换设备，远程接入局域网的方式、设备及协议，同轴电缆、双绞线、光纤等有线传输介质的分类与特点。

3.1 以太网技术

以太网技术主要规范了计算机网络的物理层和数据链路层接口，是现有军事局域网的主流建网技术。

3.1.1 IEEE 802 标准

为了制定一个标准化的计算机局域网络协议，国际上于20世纪80年代初成立了IEEE（美国电气和电子工程师学会）局域网络标准委员会（简称IEEE 802委员会）。该委员会已对计算机局域网络协议制定了若干标准。

IEEE 802标准将对应于原理体系结构模型的数据链路层划分为两个子层：逻辑链路控制子层（LLC）和介质访问控制子层（MAC），如图3-1所示。

逻辑链路控制子层（LLC）的主要功能：提供一个或多个相邻层之间的逻辑接口。

介质访问控制子层（MAC）的主要功能：

（1）发送时将数据组装成带有地址字段和差错校验字段的帧；

（2）接收时拆卸帧，即将数据帧解除封装，进行地址识别和差错校验；

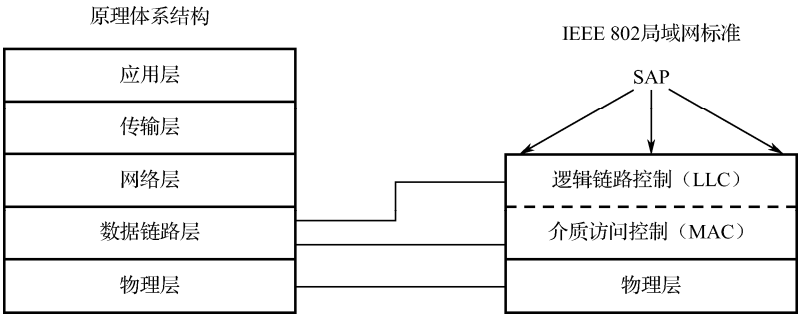


图 3-1　原理体系结构与 IEEE 802 标准的对应关系

（3）管理链路上的通信。

IEEE 802 标准针对不同的传输介质和不同的拓扑结构，分别定义了不同的 MAC 标准。如图 3-2 所示。

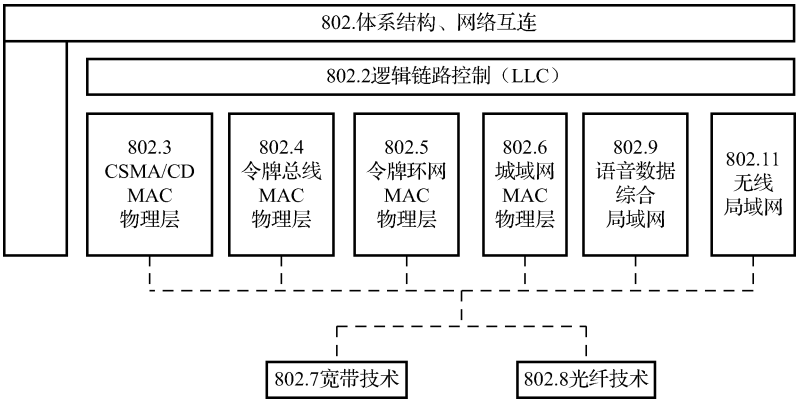


图 3-2　IEEE 802 标准系列间的关系

IEEE 802.1 的垂直部分涉及所有层，它主要提供综述、辅助信息、实用建议和指南。其水平部分涉及体系结构和网络互连。IEEE 802.2 定义逻辑链路控制标准，可以与任何一种 MAC 子层接口。

IEEE 802.3 标准主要适用于 CSMA/CD 方法，它和以太网几乎相同。这种网络价格较低，传输长度有限、网络传输效率与负载成反比。现有的标准主要针对传输速率为 10Mbps 的基带网络。

IEEE 802.4 标准适用于总线型网络中的令牌传输，即逻辑环。所采用的传输介质可以是宽带闭路电视电缆或基带电缆，或两者都采用。

IEEE 802.5 标准适用于物理环中的令牌传输，其传输介质可以是基带的双绞线或电缆。

IEEE 802.6 标准主要适用于大城市地区网络的访问控制与互连。

以太网是 20 世纪 70 年代初美国 Xerox 公司创建并由 Xerox、Intel 和 DEC 公司于 1979 年联合发布的基带局域网规范，与 1983 年正式发布的 IEEE 802.3 系列标准兼容。由于它具有结构简单、工作可靠、易于扩展等优点，得到了广泛应用。现在的以太网标准还在不断改进，其通信速度也从最初的 2.94 兆（M）位每秒、10 兆（10M）位每秒、百兆（100M）位每秒，发展到现在常见的千兆（1G）位每秒、万兆（10G）位每秒、4 万兆（40G）位每秒，10 万兆（100G）位每秒也已经出现。

3.1.2 以太网工作原理

1．CSMA/CD 协议

早期以太网多使用总线型的拓扑结构，采用同轴电缆作为传输介质。为了在广播总线上实现一对一通信，以太网采用 CSMA/CD（Carrier Sense Multiple Access with Collision Detection，带有冲突监测的载波侦听多址访问）机制进行数据传输。

当以太网中的一台主机要传输数据时，它将按如下步骤进行。

（1）侦听信道上是否有信号在传输。如果有，表明信道处于忙状态，就继续侦听，直到信道空闲为止。

（2）若没有侦听到任何信号，就传输数据。

（3）传输时继续侦听，如果发现冲突则执行退避算法，随机等待一段时间后，重新执行步骤（1）。检测到“冲突”信号的依据是导线上的电压超出了某一阈值电压。当采用曼彻斯特编码时，电压的过零点在每一比特的正中央。发生冲突时，过零点的位置将改变。根据过零点位置的变化，也可以判断是否发生了冲突。

（4）若未发现冲突则发送成功，所有计算机在试图再一次发送数据之前，必须在最近一次发送后等待若干时间（对于 10Mbps 网络，需等待 9.6μs）。

将 CSMA/CD 比作一种文雅的交谈，就是“先听后说，边说边听”。在这种“交谈”方式中，如果有人想阐述观点，他应该先听听是否有其他人在说话（即载波侦听），如果这时有人在说话，他应该耐心地等待，直到对方结束说话，然后他才可以开始发表意见。另外，有可能两个人在同一时间都想开始说话，那会出现什么样的情况呢？显然，如果两个人同时说话，这时很难辨别出每个人都在说什么。但是，在文雅的交谈方式中，当两个人同时开始说话时，双方都会发现他们在同一时间开始讲话（即冲突检测），这时说话立即终止。随机地过了一段时间后（回退），说话才开始。说话时，由第一个开始说话的人来对交谈进行控制，而第二个开始说话的人将不得不等待，直到第一个人说完，然后他才能开始说话。

除计算机以外，以太网的工作方式与上面的方式相同。首先，以太网网段上需要进行数据传送的节点对导线进行监听，这个过程就称为 CSMA/CD 的载波侦听。如果这时有其他节点正在传送数据，监听节点将不得不等待，直到传送节点的传送任务结束。如果某时恰好有两个工作站同时准备传送数据，以太网网段将发出“冲突”信号。这时，节点上所有的工作站都将检测到冲突信号。冲突产生后，涉及冲突的计算机将立即发出一个拥塞信号，以警告所有节点这时的以太网已产生冲突，并返回侦听信道状态。过了一段由标准算法生成的随机时间后，若继续监听到没有任何信息在传输，便再开始传输数据。等待时间随不同介质、不同速率的物理网络而异。

在 CSMA/CD 方式下，在一个时间段，只有一个节点能够在导线上传送数据。如果其他节点想传送数据，必须等到正在传输数据的节点传送结束后才能开始。以太网之所以称作共享介质就是因为节点共享同一根导线这一事实。

2．MAC 地址

在以太网中，硬件地址又称为物理地址或 MAC 地址。IEEE 802 标准所规定的 MAC 地址

是指计算机中固化在网络适配器（NIC）的 ROM 中的地址。

MAC 地址有 48 位，它可以转换成 12 位的十六进制数。这个数分成三组，每组有四个数字，中间以点分开。MAC 地址有时也称为点分十六进制数。为了确保 MAC 地址的唯一性，IEEE 对这些地址进行管理。每个地址由两部分组成，分别是供应商代码和序列号。供应商代码代表 NIC 制造商的名称，它占用 MAC 的前 6 位十六进制数字，即 24 位二进制数字。序列号由供应商管理，它占用剩余的 6 位十六进制数字，即后 24 位二进制数字。

为什么要使用这两种不同的地址？如图 3-3 所示，IP 地址在 IP 数据报的首部，而硬件地址则放在 MAC 帧的首部。在网络层及以上使用的是 IP 地址，而链路层及以下使用的是硬件地址。

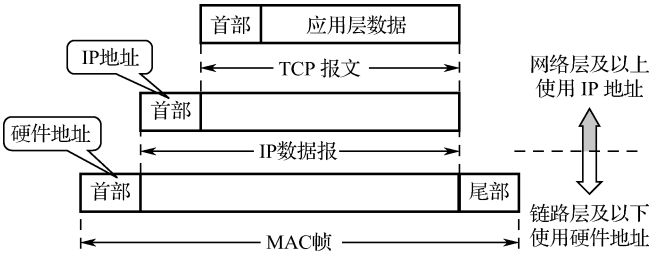


图 3-3　IP 地址与硬件地址的关系

具体的物理网络的链路层看到的只是 MAC 帧，IP 数据报被封装在 MAC 帧里面。不同的网络接口方式下，其设备标识方式、硬件地址表示方式不同，因此 IP 数据报在不同接口类型的网络上传送时，其 MAC 帧首部的内容和格式是不同的。这种变化，在上面的 IP 层是看不到的。每个路由器都有 IP 地址和硬件地址。使用 IP 地址与硬件地址，尽管连接在一起的网络的硬件地址体系各不相同，但 IP 层抽象的互联网屏蔽了下层这些复杂的细节，并使得能够使用统一的、抽象的 IP 地址进行通信。

从实际使用的角度看，以太网的 MAC 地址可以分为三类，分别是单播地址、多播地址、广播地址。

（1）单播地址：MAC 地址的第 8 位为 0，如 00e0.fc00.0006。单播地址用于网段中两个特定设备之间的通信，可以作为以太网帧的源和目的 MAC 地址。

（2）多播地址：第 8 位为 1，如 01e0.fc00.0006。多播地址用于网段中一个设备和其他多个设备通信，只能作为以太网帧的目的 MAC 地址。

（3）广播地址：48 位全 1，即 ffff.ffff.ffff。广播地址用于网段中一个设备和其他所有设备通信，只能作为以太网帧的目的 MAC 地址。

3．以太网卡的作用

以太网提供不同的 MAC 层来访问不同的物理介质。MAC 层由以太网卡实现，其主要功能是组帧、寻址、控制和维护各种 MAC 协议、定义各种媒体访问规则等。

网卡上装有处理器和存储器（包括 RAM 和 ROM）。网卡和局域网之间的通信是通过电缆或双绞线以串行传输方式进行的。而网卡和计算机之间的通信则是通过计算机主板上的 I/O 总线以并行传输方式进行的。因此，网卡的一个重要功能就是进行串行/并行转换。由于网络上的数据率和计算机总线上的数据率并不相同，因此在网卡中必须装有对数据进行缓存的存储芯片。在安装网卡时必须将管理网卡的设备驱动程序安装在计算机的操作系统中。这个驱动程序以后就会告诉网卡应当从存储器的什么位置将多大的数据块发送到局域网，或者应当在存储器

的什么位置将局域网传送过来的数据块存储下来。

网卡还要能够实现以太网协议。当网卡收到一个有差错的帧时，它就将这个帧丢弃而不必通知它所插入的计算机。当网卡收到一个正确的帧时，它就使用中断来通知该计算机并交付给协议栈中的网络层。当计算机要发送一个 IP 数据报时，就由协议栈向下交给网卡，组装成帧后发送到局域网。

3.1.3 以太网集线器与交换机

1．以太网集线器

人们在使用同轴电缆总线局域网 10BASE2 的过程中发现了它的缺点，就是当细缆总线上某个电缆接头处发生短路或开路时，整个网络就无法工作，且确定故障点相当麻烦（尤其是当总线上的站点数量很多时）。这就使得网络的可靠性很差。此外，细缆布线不够方便，价格也较高。考虑到便于维护局域网，人们又像电话网那样使用星形网拓扑，不用电缆而使用无屏蔽双绞线。每个站需要用两对双绞线，分别用于发送和接收。在星形网的中心则增加了一种可靠性非常高的设备，叫作集线器（hub）。双绞线以太网总是和集线器配合使用。由于集线器使用了大规模集成电路芯片，因此这样的硬件设备的可靠性已大大提高了。

1990 年 IEEE 制定出星形网 10BASE-T 的标准 802.3i。“10”代表 10Mbps 的数据传输速率，T 代表双绞线。但 10BASE-T 的通信距离稍短，每个站到集线器的距离不超过 100m。这种 10Mbps 速率的无屏蔽双绞线星形网的出现，既降低了成本，又提高了可靠性。10BASE-T 双绞线以太网的出现是局域网发展史上的一个非常重要的里程碑，它为以太网在局域网中的统治地位奠定了牢固的基础。

集线器的特点如下：

（1）从表面上看，使用集线器的局域网在物理上是一个星形网，但由于集线器使用电子器件来模拟实际电缆线的工作，因此整个系统仍然像一个传统的以太网那样运行。也就是说，使用集线器的以太网在逻辑上仍是一个总线网，各工作站使用的还是 CSMA/CD 协议，并共享逻辑上的总线。网络中的各个计算机必须竞争对传输媒体的控制，并且在一个特定时间至多只有一台计算机能够发送数据。因此，这种 10BASE-T 以太网又称为星形总线或盒中总线。

（2）一个集线器有许多端口，如 8～16 个，每个端口都通过 RJ45 插头（与电话机使用的插头相似，但略大一些）用两对双绞线与一个工作站上的网卡相连（这种插座可连接 4 对双绞线，实际上只用 2 对，即发送和接收各使用一对双绞线）。

（3）集线器都工作在物理层，它的每个端口都具有发送和接收数据的功能。当集线器的某个端口接收到工作站发来的数据时，就简单地将该数据向所有其他端口转发。若两个端口同时有信号输入（即发生碰撞），那么所有的端口都收不到正确的帧。

2．以太网交换机

交换机是一种基于 MAC 地址识别、能完成封装转发数据包功能的网络设备。在局域网中，交换机是用来将其他网络设备连接起来的网络设备。交换机的主要功能包括物理编址、网络拓扑结构、错误校验、帧序列及流量控制。

交换机主要采用点到点的传输方式，同一时刻可以有多个数据包进行传输。交换机之所以

能够以点对点的方式进行数据传输，是由于它的内部存储有一个 MAC 地址表，并且能够自动更新这个 MAC 地址表。交换机能记住连接到端口上的主机的 MAC 地址，形成一个端口与 MAC 地址的对应关系表，即 MAC 地址表。依据这张表，交换机从接收到的数据帧中解析出 MAC 地址，并从储存在内存中的 MAC 地址表中找出与这个数据帧中包含的目的 MAC 地址对应的端口，在这两个节点间建立起一条临时的专用数据传输通道并进行数据传输。如果在 MAC 地址表中没有找到目的节点的 MAC 地址，交换机则以广播方式分发该数据帧，此后根据目的节点发送的应答帧即可将该 MAC 地址存储到 MAC 地址表中，交换机的这种功能称为“MAC 地址学习”功能。这样，当再次需要向该节点传输数据帧时即可以点对点的方式进行传输。

以太网交换机工作在数据链路层，因此也称为二层交换机。其进行转发的依据是以太网帧中的目的 MAC 地址。交换机跟踪每个端口连接的 MAC 地址，当接收到一个以太网帧后，根据该帧的目的 MAC 地址，把报文从该目的 MAC 地址所对应连接的端口转发出去。图 3-4 为二层交换机结构示意图。

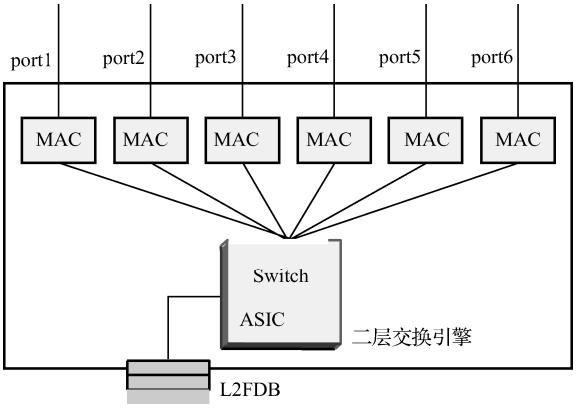


图 3-4　基于 MAC 的二层交换机结构示意图

不同交换机每个端口所能支持的 MAC 数量不同。交换机通过转发表记录 MAC 地址和交换机端口的对应关系，并存储在交换机的缓存中。如果某个端口所容纳的计算机数量超过了地址容量，则目的 MAC 地址很可能没有保存在该交换机端口的 MAC 地址表中，那么，该帧将以广播方式发向交换机的每个端口，从而被目的 MAC 地址所指的主机所接收。

交换机从端口 1 接收到一个以太网帧，其转发流程如下：

（1）根据帧的目的 MAC 查 MAC 转发表（即 L2FDB），查找相应的出端口。根据现有 L2FDB 表，报文应该从端口 2 发送出去；

（2）如果在 L2FDB 表中查找不到该目的 MAC，则该报文将通过广播的方式向交换机所有端口转发；

（3）同时该以太网帧的源 MAC 将被学习到接收到报文的端口上，即端口 1；

（4）L2FDB 表中 MAC 地址通过老化机制来更新。

交换机有直通交换和存储转发两种形式。直通交换提供线速处理能力，交换机只读出帧的前 14 字节（帧头），便将帧传送到相应的端口上，适用于全双工线路，交换速度快，但缺乏智能控制。存储转发方式要求交换机将整个帧读取到内存中，然后转发，读取整个帧虽然会增加一些延迟，但支持不同速率的端口交换，并可以校验帧数据，从而保证坏帧不会在网络上传播。

交换机的特点如下：

（1）以太网交换机的每个接口都直接与主机相连，并且一般都工作在全双工方式；

（2）交换机能同时连通多对接口，使每一对相互通信的主机都能像独占通信媒体那样无碰撞地传输数据；

（3）以太网交换机由于使用了专用的交换结构芯片，其交换速率较高。

交换机与集线器有以下不同之处。

（1）集线器工作在物理层，交换机工作在数据链路层。

（2）集线器的工作机理是广播，低端的交换机都基于 MAC 地址进行交换。

（3）带宽占用方式不同。对于普通 10Mbps 的共享式以太网，若共有 N 个用户，则每个用户占有的平均带宽只有总带宽（10Mbps）的 1/N。使用以太网交换机时，虽然每个接口到主机的带宽还是 10Mbps，但由于一个用户在通信时是独占而不是和其他网络用户共享传输媒体的带宽，因此对于拥有 N 对接口的交换机，其总容量为 N×10Mbps。这正是交换机的最大优点。

（4）集线器只能采用半双工传输模式进行传输，而交换机则不一样，它可采用全双工传输模式来传输数据，因此在同一时刻可以同时进行数据的接收和发送，数据帧处于并行状态。

3．交换机的分类

交换机按照其连接覆盖范围可分为两种：局域网交换机和广域网交换机。局域网交换机应用于局域网络，用于连接终端设备，如服务器、工作站、集线器、路由器和网络打印机等网络设备，提供高速、独立的通信通道；广域网交换机主要应用于城域网互连、广域网接入等领域，提供通信应用的基础平台。

（1）按技术类型分类

交换机可分为以太网交换机、ATM 交换机、令牌环交换机、FDDI 交换机等。现有绝大多数局域网均采用以太网交换机，进一步又可分为传统以太网交换机、快速以太网交换机、千兆位以太网交换机、万兆位以太网交换机。令牌环交换机和 FDDI 交换机已较少使用。

（2）按应用规模分类

交换机可分为企业级交换机、部门级交换机和工作组交换机、桌面型交换机四种。企业级交换机属于高端交换机，一般采用模块化的结构，它通常用于企业网络的顶层，能支持 500 个以上的节点。部门级交换机面向部门级网络，配置固定或模块化配置，一般除了常用的 RJ-45 端口外，还带有光纤端口，并支持基于端口的 VLAN（虚拟局域网），可任意采用全双工或半双工传输模式。工作组或桌面型交换机则用于用户较少的、速率为 10Mbps 或 100Mbps 的普通以太网。

（3）按端口结构分类

交换机可分为固定端口交换机和模块化交换机两种。固定端口就是它所带有的端口是固定的，硬件不可升级。模块化交换机又称为机箱式交换机，可根据不同的需要配置不同的模块，模块可以插拔，主要用于骨干网络。

（4）按协议层次分类

交换机可分为第二层交换机、第三层交换机和第四层交换机。工作层次越高，性能也越好，档次越高。二层交换机工作于数据链路层，是最原始的交换技术产品。三层交换机工作在网络层，是传统交换机与传统路由器的结合产品，既可完成传统交换机的端口交换功能，又可完成部分路由器的路由功能，并可划分 VLAN 网段，以减小广播所造成的影响。四层交换机工作于传输层，实际中较少应用。

（5）按网络管理能力分类

交换机可分为“网络管理型”和“非网络管理型”两大类。网络管理型交换机提供基于终端控制口（Console）、基于 Web 页面及支持 Telnet 远程登录等的多种网络管理方式，支持对工作状态、工作模式进行本地或远程监控管理，具有端口监控、划分 VLAN、设置 Trunk 端口等普通交换机不具备的功能。非网络管理型交换机不支持网络管理功能，无须配置即可使用。

不同网络交换机之间并不是通用的，因为使用的帧格式是不同的。如果两种类型的网络要实现互连，必须使用同时带有这两种网络类型的交换模块的交换机或路由器。

4．交换机的配置

一般情况下，交换机不需要进行特别的软件和硬件设置。不过如果想设定交换机的某些状态，如打开或关闭某个端口、划分 VLAN 等，就需要进行设置。对于不同品牌、不同系列的交换机来说，配置方式是不同的，有的使用命令行方式，有的则使用图形化界面方式。

交换机的配置需要借助计算机才能够实现。实现配置用的计算机与交换机之间的连接方法有两种：一种是通过 Console 端口直接连接的方式；另一种是通过网络接口间接连接的方式。

3.1.4　以太网的分类

1．共享式以太网

所有的以太网都遵循 IEEE 802.3 系列标准，下面列出的一些以太网络标准，前面的数字表示传输速度，单位是“Mbps”，最后的一个数字表示单段网线长度（基准单位是 100m），Base 表示“基带”的意思，T 代表“双绞线”，F 代表“光纤”。

最早的以太网就是共享式以太网，使用以下两种同轴电缆连接。

10Base5：粗同轴电缆（5 代表电缆的字段长度是 500m）。

10Base2：细同轴电缆（2 代表电缆的字段长度是 200m）。

在共享式以太网中，所有主机都以平等的地位连接到同轴电缆上，但如果以太网中主机数目较多，则存在严重的问题，如介质可靠性差、冲突严重、广播泛滥、无任何安全性。

2．标准以太网

标准以太网（10Mbps）通常只定位最终用户和接入层交换机之间的连接。由 IEEE 802.3 标准所规范，采用 CSMA/CD 协议，对于拓扑结构、传输介质、数据编码方式、数据传输速率、数据帧的长度等均有详细的描述。

按使用的传输介质不同，可分为四种。

10Base-5：粗同轴电缆，最大传输距离为 500m。

10Base-2：细同轴电缆，最大传输距离为 185m。

10Base-T：双绞线，最大传输距离为 100m。

10Base-FL：长波多模光纤，最大传输距离为 2000m。

20 世纪 80 年代末期，非屏蔽双绞线（UTP）出现并迅速得到广泛应用。UTP 的巨大优势在于：价格低廉、制作简单、收发使用不同的线缆。

3．快速以太网

快速以太网由 IEEE 802.3u 标准所规范，仍基于 CSMA/CD 技术。能够为桌面用户及服务器或服务器集群等提供 10/100Mbps 的自适应连接，也可以提供接入层和汇聚层交换设备间的连接，提供汇聚层到核心层交换设备间的连接。

快速以太网通常采用双绞线作为传输介质，也可采用“SC”接口的光纤，具体可分为以下三种。

100Base-T4：3、4 或 5 类 UTP 或 STP 双绞线（4 对线全用），最大传输距离为 100m。

100Base-TX：5 类 UTP 或 STP 双绞线（只用两对），支持全双工数据传输，最大传输距离为 100m。

100Base-FX：支持全双工数据传输，特别适合有电气干扰的环境、较大距离连接，或高保密环境等的军事网络。单模光纤最大传输距离为 2～20km，多模光纤最大传输距离为 550m～2km。

快速以太网也支持标准以太网 10Mbps 的工作方式，有良好的向下兼容性。

4．千兆位以太网

千兆位以太网将快速以太网的传输速率提高了 10 倍，达到了 1Gbps，是核心骨干网络的有效解决方案。千兆位以太网标准为 IEEE 802.3z（光纤和铜缆的全双工链路标准）和 IEEE 802.3ab（双绞线的半双工链路标准）。现在的接入层一般不使用千兆位以太网标准。许多汇聚层的以太网交换机提供千兆位接口，用于连接高速服务器或接入层交换机，许多支持堆叠功能的以太网交换机也是采用千兆位接口实现堆叠功能的。

所谓堆叠，是指通过软/硬件的支持，将一组交换机连接起来作为一个对象加以控制的方式，通常有菊花链模式和星形模式。其最大优点在于可实现简单的本地管理，但由于是一种非标准技术，通常不支持各个厂家交换机的混合堆叠。

千兆位以太网的传输介质以“SC”接口的光纤和“RJ45”接口的双绞线为主，具体分为以下七种。

1000Base-T：5 类 UTP 双绞线（4 对线全用），最大传输距离为 100m。

1000Base-CX：使用 9 芯 D 形连接器连接两对特殊 STP 铜缆，最大传输距离为 25m。

1000Base-SX：62.5/125MMF，短波，最大传输距离为 260m。

1000Base-SX：50/125MMF，短波，最大传输距离为 525m。

1000Base-LX：62.5/125MMF，长波，最大传输距离为 550m。

1000Base-LX：50/125MMF，长波，最大传输距离为 550m。

1000Base-LX：9/125SMF，长波，最大传输距离为 3000～5000m。

千兆位以太网协议遵从许多原始的以太网规范，所以可应用现有的知识和技术进行安装、管理和维护千兆位以太网。

5．万兆位以太网

万兆位以太网由 IEEE 802.3ae 标准所规范，采用全双工模式。目前主要用于大型网络（如城域网、数据中心等）的骨干部分，采用的传输介质为光纤，兼容同步光纤网络（SONET）的传输格式。

10GBase-SR 和 10GBase-SW：短波（850nm），多模光纤（MMF），光纤距离为 2～300m。
10GBase-LR 和 10GBase-LW：长波（1310nm），单模光纤（SMF），光纤距离为 2m～10km。
10GBase-ER 和 10GBase-EW：超长波（1550nm），单模光纤（SMF），光纤距离为 2m～40km。

3.2 VLAN 虚拟局域网技术

VLAN（Virtual Local Area Network，虚拟局域网）是交换机相比集线器引入的一个新技术。交换机上运行的软件可以设置连接系统的参数，按工作组设置而不是按地区设置。VLAN 将一组位于不同物理网段上的计算机从逻辑上划分成不同的逻辑网段，虚拟的局域网可以跨过多个物理网段，其功能和使用与传统 LAN 基本相同，但通信流已从多个物理网段分开，从而保持在自己的虚拟网中，如图 3-5 所示。

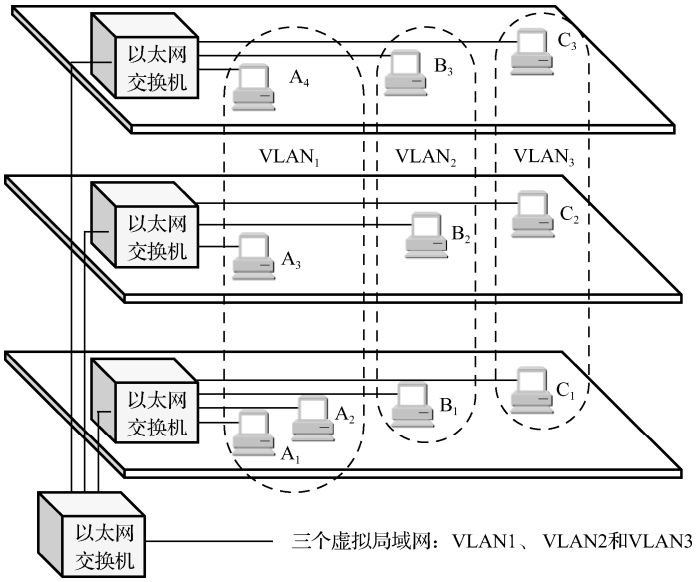


图 3-5　VLAN 示意图

VLAN 与使用交换机构成一般逻辑子网的最大区别就是不受地理位置的限制，即构成 VLAN 的节点可以位于不同的物理网段中。同一个 VLAN 的节点所发出的数据可以广播传输到该 VLAN 的所有节点，而不同 VLAN 的节点的数据不能直接广播传输，这有助于控制网络流量、减少设备投资、简化网络管理。

1．VLAN 的好处

（1）限制网络中的广播

支持 VLAN 的交换机可以形成更小的广播域或逻辑网段，有效隔离 VLAN 间的广播数据，减少 VLAN 中广播数据的通信量。这如同工作在第三层的路由器所具有的广播“防火墙”功能。

（2）虚拟工作组

使用 VLAN 的另一个目的就是建立虚拟工作组。VLAN 内的某一个成员移动到另一个网

络位置时，它所使用的工作站不需要做任何改动，仍可与原 VLAN 成员构成“局域网”。也可以将来自不同物理网络的各部门计算机组建成“一个办公室”的虚拟网络。

（3）安全性

一个 VLAN 的数据包不会发送到另一个 VLAN，这样就可以有效隔离 VLAN 间的访问，确保某 VLAN 的信息不会被其他 VLAN 的用户窃听，从而实现了信息保密。但如果要完全隔离两个网段，还是要用两个物理交换设备。

（4）减少移动和改变的代价

用户从一个位置移动到另一个位置时，其网络属性不需要重新配置或修改，通过采用恰当的 VLAN 划分方法即可动态接入新的网络，这种能力在移动组网系统中非常有用。

2．VLAN 的划分方法

（1）根据端口定义

许多交换机都可用端口来划分 VLAN 成员，被设定的端口都在同一个广播域中。例如，通过把每个情报终端连接的交换机端口指定为同一工作组，可以生成虚拟局域网，其内部用户可以相互独立地工作和使用服务器。如图 3-6 所示，交换机上的端口被划分成了“指挥用户”、“情报用户”、“互连设备”3 个 VLAN。

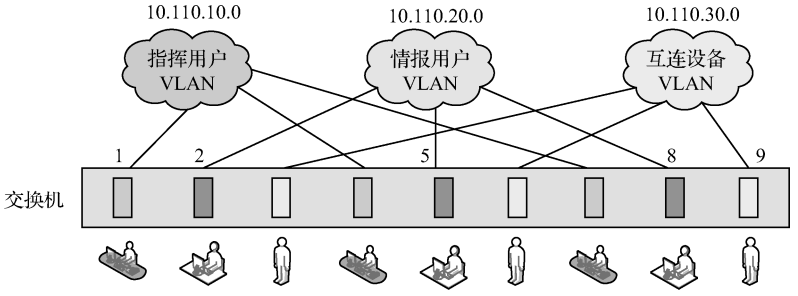


图 3-6　基于端口划分 VLAN

这样，VLAN 内部之间的通信保持在组中，而 VLAN 之间的通信流是分开的，阻止了广播通信流，有助于减少不必要的通信流。

按交换机端口划分 VLAN 成员配置过程简单，是最常用的静态 VLAN 划分方式。但是，这种方式不允许多个 VLAN 共享一个物理网段或交换机端口，而且，如果某一个用户从一个端口所在的虚拟局域网移动到另一个端口所在的虚拟局域网，网络管理者需要重新进行配置，这对于拥有移动用户数量较大的网络来说比较麻烦。

（2）根据 MAC 地址划分 VLAN

这是根据每个主机的 MAC 地址来划分的，即对每个 MAC 地址的主机都配置它属于哪个组，因此需要事先为交换机配置主机 MAC 地址与 VLAN 的映射关系数据库。这种 VLAN 划分方法的优点就是当用户物理位置移动时，即从一个交换机换到其他交换机时，VLAN 不用重新配置，所以这种根据用户 MAC 地址划分的 VLAN 也称为动态 VLAN。

这种方法的缺点是：初始化时所有用户都必须进行配置，如果有几百个甚至上千个用户，配置比较费时；而且这种划分方法也可能会降低交换机效率，因为交换机的每个端口都可能存在多个 VLAN 的成员，这样就无法限制广播包。

（3）根据网络层划分 VLAN

这是根据每个主机的网络 IP 地址或协议类型（如果支持多协议）划分的。这种方法的优点是用户的物理位置改变了，不需要重新配置它所属的 VLAN，也不需要附加帧标签来识别 VLAN，这样可以减少网络的通信量。但效率相对于前面两种方法较低，因为需要花费时间检查每一个数据包的网络层地址。

（4）IP 组播作为 VLAN

IP 组播实际上也是一种 VLAN 的定义，即认为一个组播组就是一个 VLAN，这种划分方法将 VLAN 扩大到了广域网，因此具有更大的灵活性，而且更容易通过路由器进行扩展，当然这种方法不适合局域网，主要是效率不高，对于局域网的组播，有二层组播协议 GMRP。

（5）基于组合策略划分 VLAN

即上述各种 VLAN 划分方式的组合。目前很少采用这种 VLAN 划分方式。

3．VLAN 的转发流程

如图 3-7 所示，VLAN 帧格式就是在原来以太网帧的源 MAC 地址之后加入了包含 VLAN ID 的 4 字节 VLAN TAG Header，称为 VLAN 标记，用来指明发送该帧的计算机属于哪个虚拟局域网。

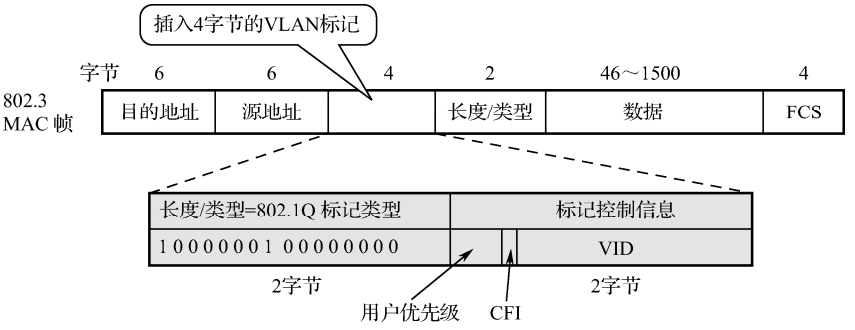


图 3-7　VLAN 的 MAC 帧格式

例如，在军事信息系统中，可以将每类业务系统划分为一个独立的 VLAN 来进行二层隔离，需要互通的业务通过三层交换来实现。VLAN ID 划分如表 3-1 所示。

表 3-1　VLAN ID 划分

VLAN 分类	业 务 类 型	VLAN ID	备　　注
用户接入 VLAN	指挥	100～199	
	情报	200～299	
	语音	300～399	
	视频会议	400～499	
	其他	500～599	默认 500
设备互连 VLAN	核心上连与互连	601～699	链路排序
		600	核心互连
设备互连 VLAN	汇聚上连与互连	701～799	链路排序
		700	汇聚互连
	接入上连	801～899	链路排序

通过设定连接交换机之间的链路为支持传送 VLAN Tag Header 的 Trunk 链路，很容易实现前面提到的虚拟工作组功能，如图 3-8 所示。交换机 A、B 上的端口分别属于指挥用户 VLAN、情报用户 VLAN、互连设备 VLAN，通过 Trunk 链路可以使得分别接在交换机 A、B 上的指挥 VLAN 用户之间进行通信；情报用户 VLAN、互连设备 VLAN 也是如此。

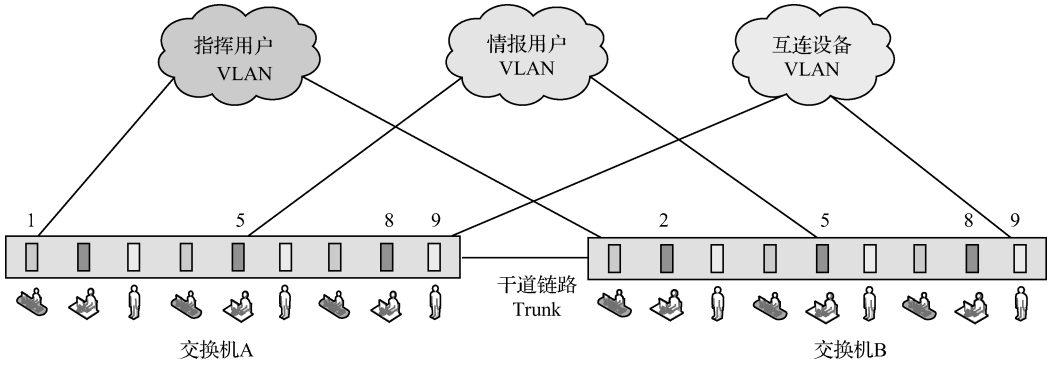


图 3-8　Trunk 链路实现虚拟工作组

一般来说，用户终端是不支持 VLAN 识别的。因此，在由 VLAN 构建的二层交换网络中，存在两种类型的链路。

（1）Access 链路：用于接入用户终端和工作站。帧在 Access 链路上转发不带 VLAN Tag。

（2）Trunk 链路：用于支持虚拟网络技术的交换机或路由器之间的级联，连接多个虚拟局域网，允许不同设备间相同 VLAN 内的用户通信。帧在 Trunk 链路上转发带 VLAN Tag，因此允许多个 VLAN 的帧在 Trunk 链路上转发。交换机 Trunk 端口接收到以太网帧后，需要判断该 Trunk 端口是否允许帧中 VLAN ID 对应的 VLAN 通过。若允许，则进行转发；否则直接丢弃该帧。

支持 VLAN 的交换机的转发流程与普通交换机的转发流程最大的区别在于：报文在支持 VLAN 交换机内转发时都是带着 VLAN Tag 进行的。也就是说，转发过程中除了要根据 MAC 地址查找出端口外，还要判断 VLAN ID 信息。因此，支持 VLAN 交换机的交换引擎与一般交换机有所不同，如图 3-9 所示。

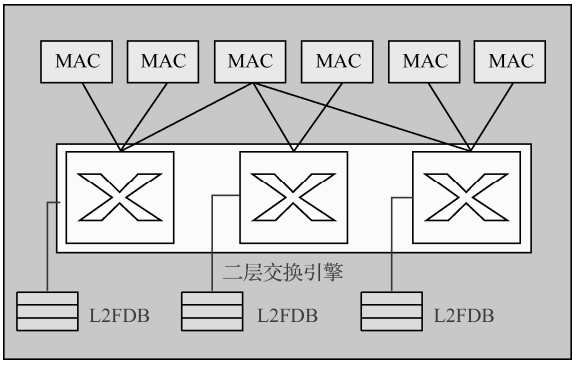


图 3-9　支持 VLAN 交换机的交换引擎

3.3 网络接入技术

军事局域网或计算机终端远程接入主干网络主要有两种方式：一种是通过路由器由光纤和光端机接入网络，满足大容量的信息传输要求；另一种是利用调制解调器进行拨号入网，通过电话线或专线接入网络，用于快速机动及不具备宽带通信条件的场合。军事局域网络的典型接入方式如图 3-10 所示。

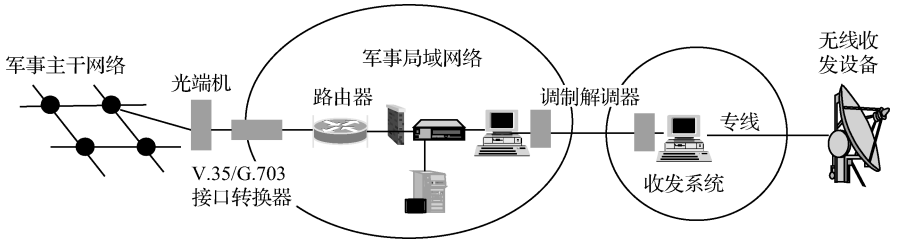


图 3-10　军事网络典型接入方式

严格地讲，主干网和本地接入网是有区别的。主干网的特点：设施共享；高度综合集成，可应付高密度的业务需求量；工作在可控环境；使用率高；技术演进迅速，以软件为主。本地接入网的特点：设施专用，且分散独立；接入业务种类多，业务量密度低；线路施工难度大，设备运行环境恶劣；使用率低；技术演进迟缓，以硬件为主；网速不一，成本与用户有关。

3.3.1　网络接入方式

1．光纤入网

光纤通信主要借助已有的网络交换、路由设备和通信接入设备，以光纤进行互连。光纤入网的连接如图 3-11 所示。

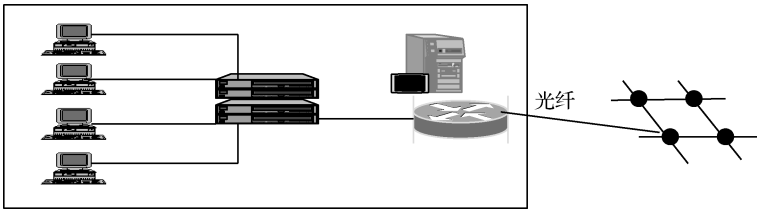


图 3-11　军事网络光纤接入示意图

低速率光纤入网采用 HDLC 或 PPP 协议方式，物理层使用 V.35 和 G.703 接口。高速光纤一般在主干交换节点接入，入网采用 SDH 方式，使用 POS 光接口。

SDH 光纤网络为用户提供最低 2Mbps 速率的接口，可满足军事信息的传输要求。目前，SDH 光纤网络的传输速率已达 10Gbps，更高速率的波分复用（WDM）及密集波分复用（DWDM）技术逐渐成熟，160Gbps 速率的波分复用传输设备已经实用化。同时，新一代光纤材料、光通信器件和全光网技术正在加紧研究，速率更快、传输性能更好的光通信网络是未来发展目标。

2．拨号入网

电话网是普及率高且廉价的通信资源。由于程控交换机的普及，国内民用电话线路已能支持相当高的数据传输速率，已能满足机动及普通信息源、机动信息用户的需求。

拨号入网作为备用或补充手段，为临时用户或无法使用光纤入网的用户提供低速连接的方法。使用拨号入网的用户可以是一台计算机，也可以是一个计算机网络。单台计算机使用拨号入网的连接如图 3-12 所示。军事网络拨号接入示意图如图 3-13 所示。

图 3-12　单台计算机拨号入网示意图

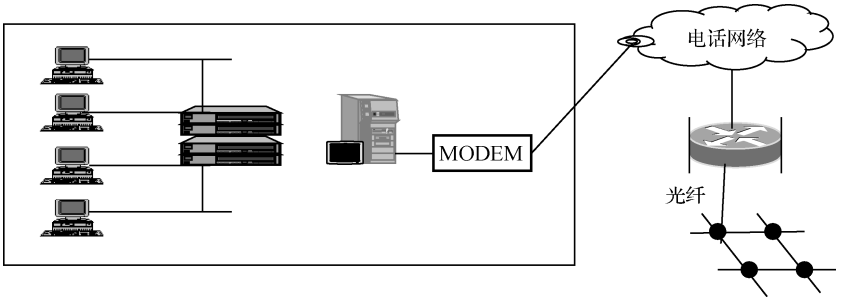


图 3-13　军事网络拨号接入示意图

拨号入网必须使用 MODEM——调制解调器。拨号入网采用 SLIP/PPP（Serial Line IP Protocol/Point to Point Protocol）协议方式，物理层使用 RS-232C 接口。SLIP/PPP 就是在串行线路上实现 IP 分组传输，因此完整的 TCP/IP 可以运行在拨号线或专线上，这给使用低速线路的远程网络级互连提供了极大的方便。由于省掉了一对路由器线路，也降低了成本，这在报文流量不是很大的军事系统中是很好的选择。

3．数据链入网

数据链也是一种信息分发系统，是一种信息输入/输出手段。对于机动入网设备，还须利用相应的数据链进行信息传输。数据链接入方式如图 3-14 所示，用户可直接接入或通过网络节点接入，主要采用 G.703 和 RJ45 网络接口。

3.3.2　网络接入设备

1．调制解调器

基于电话网使用拨号入网必须使用调制解调器（又称 MODEM）。计算机可以通过它进入公用电话网或专网与相距甚远的计算机进行数据传输，也就是说，调制解调器可以利用现有的电话线将数据传送到远端，如图 3-15 所示。发送数据的源设备或目的设备称为数据终端设备（DTE），包括计算机和数据终端。调制解调器就是一种常用的数据通信终端设备（DCE）。

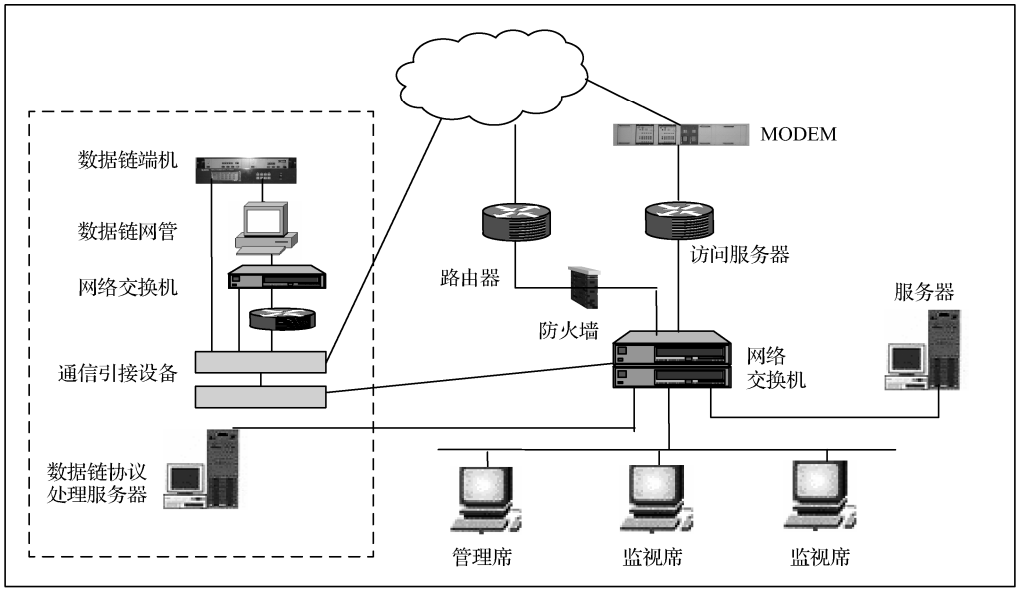


图 3-14　数据链与军事网络的互连

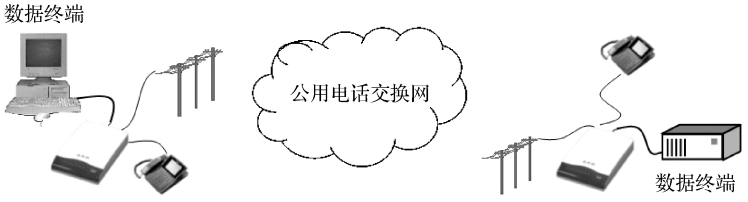


图 3-15　调制解调器连接示意图

调制解调器是计算机终端或小型局域网接入广域网的数据传输设备。调制解调器将数字信号与模拟信号相互转换，具有调制和解调两方面的功能。调制是将计算机输出的数字信号转换成可在电话网络中传输的模拟信号；解调是将电话网络上传输的模拟信号转换成计算机可识别的数字信号。调制解调器主要用于电话网络（PSTN）连接的计算机之间的通信。

（1）调制解调器的工作模式

调制解调器加电后，具有两种工作模式：命令模式和数据模式。

① 命令模式：调制解调器可接收来自设置面板的操作命令或来自终端的 AT 命令，并根据命令执行相应的操作。

② 数据模式：调制解调器可通过线路（交换线或专线）与远端调制解调器和终端交换数据信息，此时本地终端发送的数据（包括命令）均被视为用户信息经电话线传送到远端。

调制解调器可以通过命令设置，使它工作在专线和交换线方式下。

（2）调制解调器的连接方式

① 专线：指为使用者提供一条专属的通信线路，不经过程控交换机，线路的各个端点都固定不变，可每天 24 小时连续使用，并提供绝对的保密性，任何这条线路外的单位都无法切入此线路。因为线路是固定的，所以线路质量较好，并且较为稳定。专线又分为二线式与四线式两种。四线式利用两条线供单方向传输，另外两条线作反方向传输，从而达成全双工的功能。二线式则只使用两条线，同时做双向接收/发送工作，利用接收/发送使用不同频率或回音消除

技术。四线式专线的质量明显优于二线式，但线路费用高于二线式，各有利弊，多数调制解调器既能工作于二线式，也能工作于四线式。

② 交换线：调制解调器需要通过拨接对方的电话号码，在对方的调制解调器应答后，才可以联机工作。例如电话、传真线路皆为交换线。由于使用广泛，对需要与不定对象交换信息时比较方便，但由于需要先执行拨号程序（约 45～60s），甚至拨不通，效率不高。每次拨通的线路不定，线路质量较差且不稳定，保密性也较差。

调制解调器能支持的终端速率为 300bps、600bps、1200bps、2400bps、4800bps、7200bps、9600bps、12000bps、14400bps、19200bps、38400bps、57600bps 和 115200bps。在大型联网军事信息系统中，中心系统一般采用机架型 MODEM（即 MODEM 池），与其异地子系统进行互联，作为应急传输线路，如图 3-16 所示。

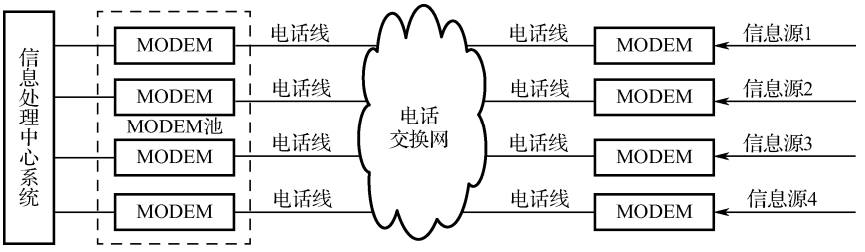


图 3-16 基于调制解调器池的有线通信网连接示意图

对于短波等无线传输手段，也有专门的调制解调器，但其收发功能是分开的，而且分无线调制解调器和有线调制解调器两种。其配置如图 3-17 所示。

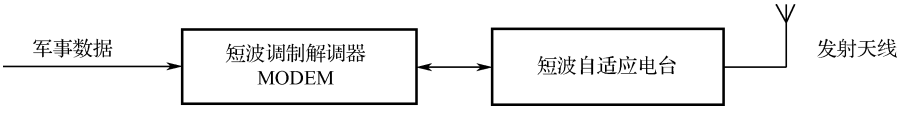


图 3-17 短波通信配置示意图

2．光端机

光纤通信系统是以光波为载体、以光纤为传输介质的通信系统，与双绞线、同轴电缆、短波通信等相比，在安全性、可靠性等方面有很大的提高，因而被广泛用来将军事局域网接入到广域网中。

光纤通信系统由光缆线路和系统设备两部分组成。系统设备由发端电端机、发端光端机、光缆、光中继器、收端光端机、收端电端机及辅助工作系统（供电系统、监控系统、勤务系统）组成。在进行长距离信息传输时还需要光中继器，其作用是将光信号转换成电信号，并进行放大，然后将电信号转换为光信号发送出去。

（1）光纤通信模型

最基本的光纤通信系统由数据源、光端机和光学信道组成，如图 3-18 所示。光端机也称光纤多路复用器，负责光电转换、光发射、光接收及信道复用传输，因此又分为光发送机和光接收机。光发送机中装有发光二极管或激光二极管，通电时可将电信号转变成适合光纤传输的光束（光信号），分内、外两种调制方式，内调制输出的光强度随信号电流变化，外调制输出的光强度随信号电压变化；光接收机内装有光电二极管，遇光就会产生电脉冲，因此光接收机负责从光纤上接收光信号，然后转变成电信号，从而还原为相应的语音、图像、数据等信息。

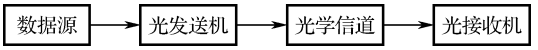


图 3-18　基本光纤通信系统示意图

（2）光端机的分类

光端机从传输方式上可分为模拟光端机和数字光端机，从对光源的调制方式上分，光发射机有直接调制型和外调制型等。各种类型的光端机都是实现将电信号变换为光信号、将光信号变换为电信号的设备。

（3）模拟光端机与数字光端机

模拟光端机将要传输的信号进行幅度、频率或相位调制，根据调制方式的不同分别称为调幅、调频、调相光端机，然后将调制好的电信号转换成光信号。在接收端将光信号还原成电信号，再把这个信号进行解调，还原出图像、语音或数据信号。

数字光端机将所要传输的信号进行数字化处理，再将这些数字信号进行复用处理，使多路低速的数字信号转换成一路高速信号，并将这一信号转换成光信号。在接收端将光信号还原成电信号，还原的高速信号分解出原来的多路低速信号，最后将这些数据信号还原成用户数据。

光端机是一种典型的数字复用设备和数据传输设备。模拟光端机采用频分复用，复用最多 4 路数据或 4 路音频。不能同时复用 4 路数据和 4 路音频，而且调试困难，交调干扰严重。而数字光端机充分利用光纤频带宽、容量大的特性，用一个波长可传输 8 路视频（1.5Gbps 带宽。如果为 3Gbps 带宽，则一个波长可传输 16 路视频），并且很容易进行大容量复用而不会相互干扰。

（4）光端机入网接口

使用光端机可以延伸E1和以太网连接范围。光纤入网采用PPP方式入网，物理层使用V.35、G.703 接口。主干交换节点一般以 155Mbps 光缆接入，入网采用 SDH 上跑 IP 协议的方式，用 POS 光接口。光端机可以在长达 120 千米的光纤线路上承载 4 条 E1、T1 线路或以太网，以及高速数据业务。图 3-19 是某光端机背板接口图。

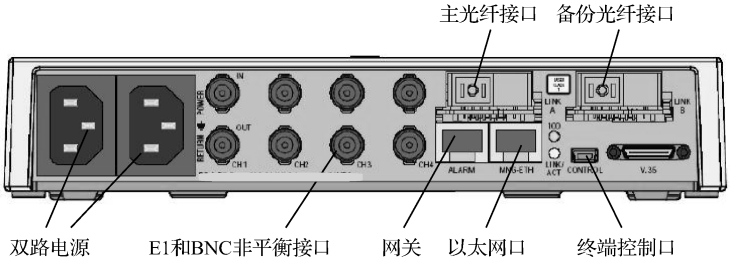


图 3-19　某光端机背板接口图

使用超级终端方式或 Web 方式，可以配置光端机的 IP 地址、子网掩码和网关，环测线路，查看接口状态。

3．接口转换器

随着现代通信技术和网络技术的不断发展，电信传输网和数字数据网之间的关系越来越密切，用电信网承载数据网络的业务，或者用数据网承载语音业务。电信服务商或其他网络接入者通常提供 E1 信道（2.048Mbps）租用链路，而许多路由器并不具备 E1 接口，为此需要一个

转换设备，实现路由器的广域网 V.35 接口信号与 E1 信道接口之间的适配转换，此类设备也可称为接口转换器（CSU/DSU，通信服务单元/数据服务单元），如图 3-20 所示。

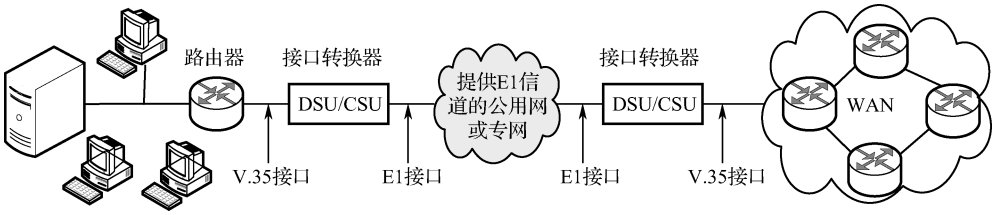


图 3-20　接口转换器典型应用示意图

接口转换器广泛应用于广域连网，多用于路由器之间的互连，或其他具有 V.35 接口的数据设备的互连。可将来自 V.35 接口的信号转换成速率为 2048Kbps 的 G.703 信号并从 E1 接口输出，或者将来自 E1 接口的信号还原成 V.35 信号。V.35 接口的速率和工作方式可选择设置。图 3-21 为接口转换器后面板。

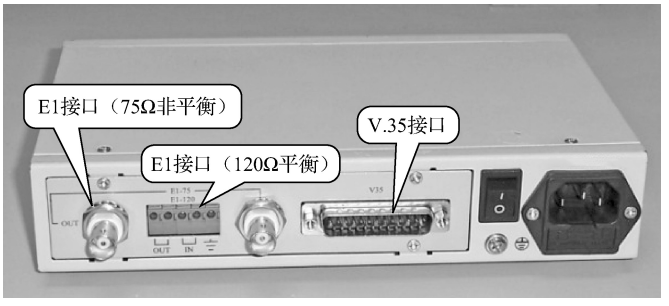


图 3-21　接口转换器后面板

接口转换器有以下两种典型应用。

（1）两个路由器通过端到端的 E1 信道互连

两端的路由器均作为数据终端设备 DTE，而接口转换器作为数据通信设备 DCE。可将传输速率设置成 2048Kbps，但速率越高，V.35 电缆的允许长度越短。

（2）路由器通过 E1 信道连接到 DDN 网

路由器通过接口转换器为 DDN 网提供远程连接。与端到端 E1 连接不同，传输速率通常需同步于 DDN 信道，速率为 64Kbps×2n（0≤n≤5），接口类型通常为 DCE。路由器和接口转换器的数据传输速率都必须依照所租用的 DDN 信道速率设置，多数路由器的传输速率根据数据通信设备接口（DCE）的速率自动调整。

4．RJ45 航空插头

以太局域网的普及和应用给军工业特别是武器装备制造业带来了巨大的变革，信息技术的发展为这些行业的工作效率和生产质量带来了前所未有的提高。然而，传统的以太网是在办公环境中使用设计的，并非针对恶劣的工业生产环境设计的，常规的商业布线系统很难适用于恶劣环境下的应用。

当局域网应用于非办公环境和恶劣环境时，会带来一系列问题。局域网的传输不仅要面临数据传输速度的问题，还面临不稳定的温度、湿度环境、油污、灰尘、腐蚀性化学物质及震动、电磁干扰等问题。因此，军工行业中对担负网络连接和传输任务的连接设备提出了适应恶劣环

境、安全牢固、防水防尘等新的要求。

航空插头也叫作军工插头，其实质是电连接器，即电缆接插件，芯数不等，大小多样。但基本都是金属壳，插头插座都有螺丝扣，可以旋紧固定。因多用在飞机上而得名。RJ45 网络航空插头将标准以太网线缆（5 类、超 5 类、6 类）转换为可靠性高的、可在一定恶劣环境下使用的网线航空插头。它具有防电磁干扰、抗震、抗冲击、适应温度急变、适应大气压力变化、防尘、防水功能（防护等级可达 IP67）、不产生信号衰减，具有卡扣锁紧结构设计，使用方便等优点。RJ45 网络航空插头可用于军事系统局域网网络连接。图 3-22 所示为符合以太网协议标准的 RJ45 网络航空插头。

图 3-22　RJ45 网络航空插头

国际电工委员会的标准 IEC 60529 规定了电气设备外壳对异物侵入的防护等级。该标准中，等级数字越大表示其防护效果越好。防尘防水等级定义如表 3-2 所示。

表 3-2　防尘防水等级定义

数字	防尘等级定义	数字	防水等级定义
0	无特殊防护	0	无特殊防护
1	防止大于 50mm 之物体侵入	1	防止滴水侵入，防止垂直滴下之水滴
2	防止大于 12mm 之物体侵入，防止手指触碰	2	倾斜 15° 时，仍能防止滴水侵入
3	防止大于 2.5mm 之物体侵入，防止工具、电线或物体侵入	3	防止喷射的水侵入，水或雨水从 60° 落到外壳上无影响
4	防止大于 1.0mm 之物体侵入，防止蚊蝇、昆虫或物体侵入	4	防止飞溅的水侵入，液体由任何方向泼到外壳上均没有影响
5	防尘，无法完全防止灰尘侵入，但侵入量不影响正常工作	5	防止大浪的水侵入，用水冲洗无影响
6	防尘，完全防止灰尘侵入	6	防止大浪的水侵入，可用于船舱内环境
		7	可用于短时间内耐浸水
		8	于一定压力下长时间浸水

3.3.3　网络接入协议

从物理层所使用的通信传输信道看，军事信息的传输信道有有线电信道、光信道、短波信道、微波信道和卫星信道等。信道级物理层接口协议标准如图 3-23 所示。

G.703/G.704 符合 ITU-T 有关电话公司设备和 DTE 间的电气和机械标准，速率可达 4Mbps。V.35 是一种 ITU-T 的接口标准，用于定义网络访问设备和分组网的接口，速率可达 4Mbps。Z 接口符合 GF002-9002.1、GJB699.5-89、GJB699-89 的有关规定，用于拨号入网。

各物理接口的使用要求是：V.35/G.703 接口（N×64Kbps）用于连接需要传输业务量大于 64Kbps、小于 2Mbps 的光纤入网等接入点；STM-1/STM-4（POS 接口）用于 155Mbps/622Mbps 主干交换节点间的连接；Z 接口用于使用 RS-232C 物理层协议的拨号入网，给低速线路的远程

网络互连提供方便。

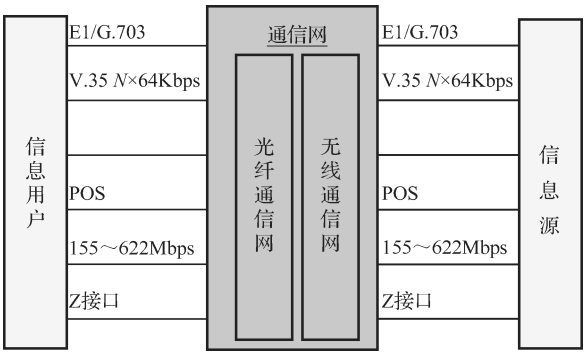


图 3-23　物理层常用接口标准

1．物理接口 E1 标准

军事网络中，E1 专用网络是地面网络的重要组成部分，主要依托传输控制设备、路由器、保密机和 E1 专线组成。它是一个与其他网络物理上完全独立的网络，具有安全、宽带可控等多种优点。

E1 电气特性符合 ITU-T G.703 建议，是我国和欧洲国家电信传输主干网使用的传输系统。E1 信号由 32 个 64Kbps 的 PCM 话路经过时分多路复用形成，速率为 2Mbps。现在常用于路由器与电话、同轴、光纤的物理连接，然后通过 PPP 数据链路协议建立起 DDN 等传输线路。

（1）E1 帧结构

在 E1 信道中，8bit 组成一个时隙（TS），由 32 个时隙组成一个帧（F），16 个帧组成一个复帧（MF）。E1 有成帧、成复帧与不成帧三种方式。在成帧的 E1 中，第 0 时隙用于传输帧同步数据，其余 31 个时隙可以用于传输有效数据；在成复帧的 E1 中，除了第 0 时隙外，第 16 时隙是用于传输信令的，只有第 1 到第 15 及第 17 到第 31 共 30 个时隙可用于传输有效数据；而在不成帧的 E1 中，所有 32 个时隙都可用于传输有效数据。

（2）E1 接口

E1 是物理连接技术，是数字网络，可以用同轴电缆也可以用光纤，然后根据用户的需要再进行信道分配，如 PPP 的 DDN 线路等都可以使用它们。

E1 接口采用非平衡的 75Ω、平衡的 120Ω两种接口。

（3）E1 接口的使用

通信双方的 E1 接口在参数上必须完全一致，才能保证物理层正常工作。E1 接口的使用有三种方法：

① 将整个 2Mbps 用作一条链路，如 DDN 2Mbps；

② 将 2Mbps 用作若干 64Kbps 及其组合，如 128Kbps、256Kbps 等；

③ 在用作语音交换机的数字中继时，这也是 E1 本来的用法，是把一条 E1 作为 32 个 64Kbps 来用，但是时隙 0 和时隙 15 是用作信令的，所以一条 E1 可以传 30 路语音。

（4）E1 和 T1 的区别

除了 E1 电路，还有 T1 电路，E1 电路主要应用在欧洲、俄罗斯、中国等世界大部分地区，T1 电路主要应用在美洲。E1 是 2.048Mbps，T1 是 1.5Mbps，这主要是由于采用不同数字压缩算法造成的。E1 用的 PCM 是 64Kbps，而 T1 用的是 56Kbps。

2．物理接口 V.35 标准

CCITT（现在叫 ITU-T，International Telecommunications Union，国际电信同盟）从 20 世纪 60 年代开始制定 V 系列建议，现在几经修订，成为一个较为全面和完善的建议。V 系列建议是为电话网上的数据通信而制定的，其中 V.35 的最初版本是 ITU-T 于 1968 年发布的。当时，随着数据通信传输速率的提高，超过音频电路 48Kbps 的传输应用越来越广泛，为了在模拟线路上解决这类问题，使得在 60～108kHz 基群电路上可以传输大于 48Kbps 速率的数据，ITU-T 制定了 V.35、V.36 和 V.37 标准，实现了 48～144Kbps 数据传输速率的宽带调制解调器，有的资料上也将 V.35、V.36 和 V.37 标准统称为 V.35 协议族。而 V.35 建议本身被看作数据传输速率在 48～64Kbps 之间的宽带模拟调制解调器和 DTE 之间的接口。

目前，随着宽带模拟调制解调器应用的逐渐减少，V.35 接口又被分组交换机、路由器和网关等数据服务单元（DSU）采用，成为当前通信设备中流行的远程高速同步接口。V.35 的传输速率也从常用的 48～64Kbps 提升到支持更高的 E1、T1、ATM 及帧中继等通信网，最高可达 6Mbps。V.35 在 100Kbps 的情况下，电缆的理论长度可以达到 1200m，实际长度要根据设备和电缆质量来确定。但需注意，路由器和接口转换器的数据传输速率必须依照 E1 支持的信道速率设置。当然，大多数路由器的数据传输速率会随接口的速率自动调整。

3．拨号连网 PPP 协议

基于电话网的拨号连网协议主要是 PPP 和 SLIP 等协议。

点到点协议（Point to Point Protocol，PPP）是在点对点线路上对 IP 分组进行中继的数据链路协议，可以运行在 RS-232、RS-422 和 V.35 等各种物理接口之上，实现路由器到路由器或主机到网络的点对点连接。

PPP 是由两种协议构成的：一种是为了确保不依存于网络协议的数据链路而采用的 LCP（数据链路控制协议）；另一种是为了实现在 PPP 环境中利用网络层协议控制功能的 NCP（网络控制协议）。NCP 从其目的出发需要在每个网络层协议都作规定。NCP 的具体名称在对应的网络层协议中有所不同。更准确地说，PPP 所规定的协议只是 LCP，至于如何将 NCP 及网络层协议放入 PPP 帧中，要由开发各种网络层协议的厂家解决。PPP 帧具有传输 LCP、NCP 及网络层协议的功能。对利用 LCP 的物理层规格没有特殊限制。

PPP 的主要功能：在同一链路上封装和传输不同的网络层协议数据报，建立、配置和测试链路层连接，建立和配置网络层协议。成帧的方法可清楚地区分帧的结束和下一帧起始，帧格式还处理差错检测；链路控制协议用于启动线路、测试、任选功能的协商及关闭连接。

ADSL 等调制解调器利用 PPP 协议进行拨号连接的工作过程如下：

（1）终端计算机通过调制解调器呼叫 ISP（Internet Service Provider，网络服务提供商）的路由器，然后路由器一边的调制解调器响应电话呼叫，建立一个物理连接。

（2）终端计算机接着对路由器发送一系列 LCP 分组，用这些分组及其响应来选择所用的 PPP 参数。

（3）当双方协商一致后，终端计算机发送一系列 NCP 分组以配置网络层（NCP 的功能就是动态分配 IP 地址），使得终端计算机可以发送和接收 IP 分组。

（4）当终端计算机的用户完成数据发送、接收功能后，不需要再连网时，NCP 用来断开网络层连接，并且释放 IP 地址，然后 LCP 断开链路层连接。

（5）终端计算机通知调制解调器断开电话线路，释放物理层连接。

PPP 是 SLIP（Serial Line IP Protocol）协议的继承者，是一种标准的串行线路封装方法。PPP 支持密码认证协议（PAP）和握手验证协议（CHAP），还支持动态地址分配、多种协议以及同步、异步通信等。串行线路互联协议（SLIP）是 UNIX 机器标准配置的广域传输协议，它面向低速串行线路封装 IP 分组，既可使用 RS-232C 连接串口线路，也可使用调制解调器连接电话网。实际上，除了用于路由器之间的连接，还可用于主机之间、主机和路由器之间的连接。

3.4 网络传输介质

网络传输介质是网络中传输数据、连接各网络节点的实体，是信息从发送方传输到接收方的物理路径。网络传输介质分为有线传输介质和无线传输介质两大类。目前常见的有线传输介质有同轴电缆、双绞线和光缆 3 种。其中，同轴电缆一般用于总线型网络中；双绞线是目前最常用的传输介质，主要用于星形网络中；而光缆则主要用于主干网的连接。无线传输介质主要有红外线、微波、激光等。

对有线传输介质而言，电磁波沿着某一固体介质（如双绞线、电缆或光纤）导向传播。无线传输介质是指自由空间，它提供了传输电磁波信号的手段。下面简要介绍有线传输介质。

3.4.1 同轴电缆

同轴电缆用于传统的总线型以太网中。同轴电缆共有四层，如图 3-24 所示，由内导体铜芯线、绝缘层、网状编织的外导体屏蔽层及保护塑料管外层组成。同轴电缆具有寿命长、频带宽、质量稳定、外界干扰小、可靠性高、技术成熟等优点。但因受网络布线结构的限制，日常维护不便，故障诊断和修复比较麻烦，同轴电缆网络已基本被非屏蔽双绞线或光缆所取代。

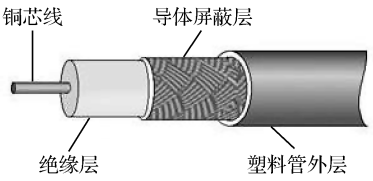


图 3-24 同轴电缆的结构示意图

根据其传输频带不同，同轴电缆分为有线电视用的宽带同轴电缆和计算机网络用的基带同轴电缆两种。

1．宽带同轴电缆

这是一种阻抗为 75Ω、直径为 0.25 英寸的宽带同轴电缆。其屏蔽层通常用铝冲压而成，用于传输模拟信号。宽带同轴电缆实际上就是有线电视（CATV）电缆，可使用的频带高达 300～450MHz。宽带系统采用频分多路复用技术，又分为多个信道，可同时传送不同频率的信号，可使数据、声音、图形及影像等在不同的频道中同时传送。但对于数据信号需要使用调制解调器。如果利用整个电缆的带宽来进行数字传输，可以达到 50Mbps 的数据传输速率。

2．基带同轴电缆

基带同轴电缆是阻抗为 50Ω的电缆，主要用于传输数字信号，用作计算机网络的传输介质。在信号传输过程中，基带同轴电缆上的传输信号将占用整个频道。因此，在同一时间内，基带

同轴电缆只能传送一种信号。基带同轴电缆的带宽取决于电缆长度。短电缆可获得较高的数据传输速率。

3.4.2　双绞线

双绞线（Twisted Pairwire，TP）是最常用的一种传输介质。它由两根相互绝缘的导线按照一定的规格以螺旋形式相互缠绕在一起而成，每根线的绝缘层有色标来标记，双绞线也因此而得名。把两根绝缘的导线按一定密度互相绞在一起，使导线在传输中辐射的电磁波相互抵消，减少了导线之间的电磁干扰，并具有抗外界电磁干扰的能力。双绞线原来主要用在电话系统中传输模拟声音信息，现在主要用于计算机网络中传输数字信号。

1．双绞线的特点

目前，组建局域网络所用的双绞线电缆一般由 4 对线（即 8 根线）组成。在双绞线电缆内，不同线对具有不同的扭绞长度。双绞线具有成本低、直径小、阻燃性、重量轻、易弯曲等优点，一般用于星形网络中，每条双绞线通过两端安装的 RJ45 连接器（俗称水晶头）与网卡、集线器或交换机相连，如图 3-25 所示。

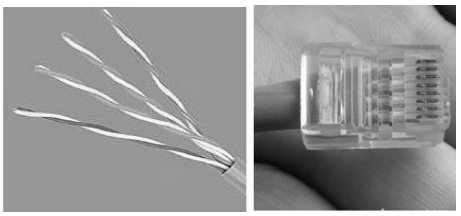


图 3-25　双绞线与水晶头

在计算机网络通信中，双绞线一般用于几百米以内的数据传输。但实际上，双绞线的传输距离可达几到几十千米，对于模拟信号每 5～6 千米需加放大器，对于数字信号每 2～3 千米需加中继器。

双绞电缆按其外部是否包裹有金属层和塑橡外皮，可分为无屏蔽双绞电缆（Unshielded TP，UTP）和屏蔽双绞电缆（Shielded TP，STP）两大类。屏蔽双绞线既有塑橡皮的护套层，又在护套层内增加了金属层，有效地减小了影响信号传输的电磁干扰，理论上 100m 内可达到 500Mbps 的数据传输速率，实际中通常使用的数据传输速率不超过 155Mbps；但相应增加了成本，且安装时要比非屏蔽双绞线电缆困难，需要支持屏蔽功能的特殊连接器和相应的安装技术。而非屏蔽双绞线只有一层塑橡护层，没有金属保护层，因而易受电磁干扰，但成本较低。电磁辐射严重、对传输质量要求较高等的场合使用屏蔽双绞线，一般场合采用非屏蔽双绞线即可传输 100m 的距离。

2．非屏蔽双绞线的规格

非屏蔽双绞线按其电气特性（即传输速率和信噪比）又可分为不同的规格。1991 年，美国 EIA（电子工业协会）的 TIA（远程通信工业分会），即通常所说的 EIA/TIA，颁布的 EIA-568 标准（即商业大楼的通信布线标准）将非屏蔽双绞线分为 5 类。随着传输介质的发展，近年来在局域网中又出现了超 5 类、6 类、7 类双绞线，传送信号时衰减更小，抗干扰能力更强，支

持更高带宽的网络应用。双绞线类别及其用途如表 3-3 所示。

这里“类”的含义是指某一类布线产品所能支持的布线等级。

1 类：主要用于 20 世纪 80 年代初之前的电话线语音传输，不用于数据传输。

2 类：传输频率为 1MHz，用于语音传输和最高传输速率为 4Mbps 的数据传输，常见于使用 4Mbps 规范令牌传递协议的旧的令牌网。

3 类：指目前在 ANSI 和 EIA/TIA 568 标准中指定的电缆。该电缆的传输频率为 16MHz，用于语音传输及最高传输速率为 10Mbps 的数据传输，主要用于 10Base-T。

4 类：该类电缆的传输频率为 20MHz，用于语音传输和最高传输速率为 16Mbps 的数据传输，主要用于基于令牌的局域网和 10Base-T/100Base-T。

5 类：该类电缆增加了绕线密度，外套一种高质量的绝缘材料，传输频率为 100MHz，用于语音传输和最高传输速率为 100Mbps 的数据传输，主要用于 10Base-T 和 100Base-T 网络，这是最常用的以太网电缆。

超 5 类或 6 类双绞线用于千兆位以太网，是市场上最常见的双绞线。

表 3-3 双绞线类别及其用途

绞合线类别	应　用
1 类	只能用于声音传输，不能用于数据传输（低于 20Kbps）
2 类	用于 0.1～2Mbps 的声音传输和小于 4Mbps 的数据传送
3 类	用于 10Mbps、10Base-T 局域网的声音传输或数据传送
4 类	用于 20Mbps、10Base-T 和 16Mbps 的令牌环网
5 类	用于 100Mbps、100Base-T 和 155Mbps ATM 高速局域网
超 5 类	用于 100Base-T 快速以太网、某些 1000Base-T 吉比特以太网
6 类	用于 1000Base-T 吉比特以太网、ATM 网络
7 类	用于 10 吉比特以太网

3．双绞线的接线标准

双绞线网线制作得是否恰当，将会影响到网络性能的发挥，甚至影响网络的正常工作。

RJ45 水晶头由金属片和塑料构成，与电话线上的 RJ11 水晶头非常相似。RJ45 水晶头的序号对网络连线非常重要，绝对不能搞错，这与它的各金属引脚在网络数据传送中所担负的任务（功能）有关。将金属引脚前端朝上面对人眼时，如图 3-26 所示，最左边的就是第“1”脚，然后往右依次为“2”、“3”……直到第“8”脚。表 3-4 描述了这 8 个金属引脚的功能或电气定义。

8 只金属引脚分为 4 个绕对或线对，即：

第 1、2 线为一个绕对，即第 1 绕对；

第 3、6 线为一个绕对，即第 2 绕对；

第 4、5 线为一个绕对，即第 3 绕对；

第 7、8 线为一个绕对，即第 4 绕对。

在 10Base-T 标准中，以太网在使用双绞线作为传输介质时，只需要 2 对（4 芯）线就可以完成信号的发送和接收。即：双绞线的第 1 绕对使用 RJ45 水晶头的第 1 引脚和第 2 引脚，第

2 绕对双绞线使用第 3 引脚和第 6 引脚，第 3 绕对和第 4 绕对备用。而在 100Base-TX 的快速以太网中需要使用 4 对线，即 8 个引脚都要用到。

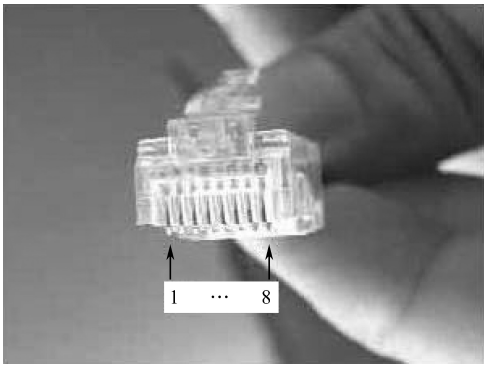


图 3-26　RJ45 水晶头金属引脚序号

表 3-4　RJ45 水晶头信号

线　序	功　能	缩 写 名	说　明
1	发送数据+	TX_D1+	
2	发送数据–	TX_D1–	
3	接收数据+	RX_D2+	
4	接收/发送数据+	BI_D3+	10Base-T 标准中未用
5	接收/发送数据–	BI_D3–	10Base-T 标准中未用
6	接收数据–	RX_D2–	
7	接收/发送数据+	BI_D4+	10Base-T 标准中未用
8	接收/发送数据–	BI_D3–	10Base-T 标准中未用

双绞线必须按一定的线序标准压在 RJ45 水晶头内。目前存在两个国际接线标准，即 T568A 和 T568B。这两个标准都规定了各自的线的排列方式，但是这二者没有本质的区别，只是在线序上略有不同而已，如表 3-5 所示。工程中常采用 T568B 标准。

表 3-5　T568A 和 T568B 标准

线　序	T568A 标准	T568B 标准
1	白绿	白橙
2	绿	橙
3	白橙	白绿
4	蓝	蓝
5	白蓝	白蓝
6	橙	绿
7	白棕	白棕
8	棕	棕

从表 3-5 可以看出，T568A 和 T568B 之间的关系只是将其 1、3 号线对调，2、6 号线对调。由此可见，两个接线标准的本质是要保证线对或绕对的正确性。

依据双绞线两端所需连接的网络设备的不同，双绞线有直通线和交叉线两种接法。

（1）直通线接法

所谓直通线接法，就是双绞线的 8 根线接在水晶头中的引脚位置要完全一致，不能出现交叉的情况。简单地说，就是双绞线两端都使用相同的接线标准，按 T568A 或 T568B 均可。图 3-27 为 T568B 标准线序示意图。

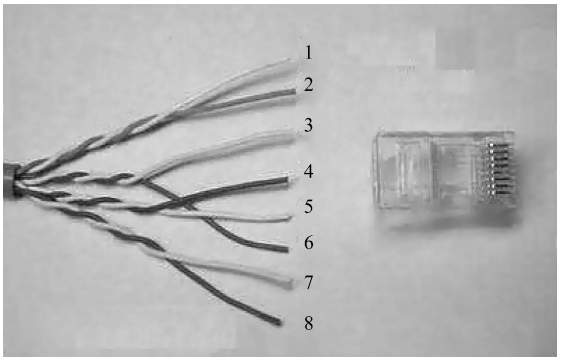


图 3-27　T568B 标准线序示意图

直通线网线用于连接不同类型的网络设备，如交换机（或集线器）Uplink 口与交换机（或集线器）普通端口的连接，交换机（或集线器）普通端口与计算机网卡的连接等。具体可分为一一对应接法和 100M 接法两种。

① 一一对应接法：双绞线的两头连线要一一对应，即一头的第 i（i=1，2，…，8）脚一定要连着另一头的第 i（i=1，2，…，8）脚。这种接线方法对线无顺序要求。

② 100M 接法：这种接法能满足 100Mbps 和 1000Mbps 带宽的传输速率。它虽然也是一一对应的，但双绞线两端水晶头的每一引脚上所接线的颜色是固定的，即两端均按 T568A 或 T568B 标准线序与水晶头相接。

一一对应接法在传输距离近、传输速率不高时能正常使用。但是因为第 3、6 信号线未绞在一起，芯线之间存在相互串扰，从而失去了双绞线的屏蔽作用。这样，当传输距离较远时会出现丢包，或者导致局域网速度慢；在 100Mbps 以上高速网络中，多采用 100M 接法。

（2）交叉线接法

顾名思义，交叉线接法是将双绞线电缆接到其两端的水晶头中时，接线有交叉，如图 3-28 所示。交叉线用于连接相同类型的网络设备，如网卡与网卡之间的连接、交换机（或集线器）普通端口与交换机（或集线器）普通端口的连接、集线器或交换机的级联等。

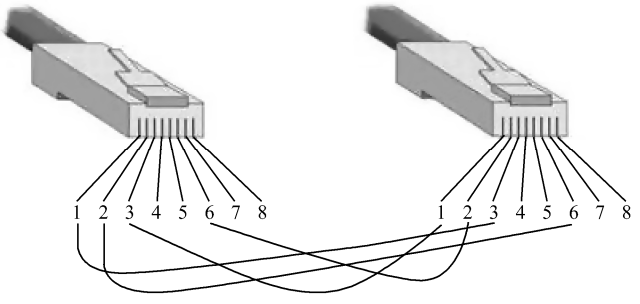


图 3-28　交叉线接法

图 3-28 中，未标识接线的第 4、5、7 和 8 脚分别一一对应相连。交叉线接法实际上就是在双绞线电缆的两端分别使用 T568A 标准和 T568B 标准。

综上所述，直通线接法就是双绞线的两头都采用 T568A 标准或 T568B 标准的接法；交叉线接法就是双绞线的一头采用 T568A 标准，而另一头采用 T568B 标准。两种连接方法的对比如图 3-29 所示。

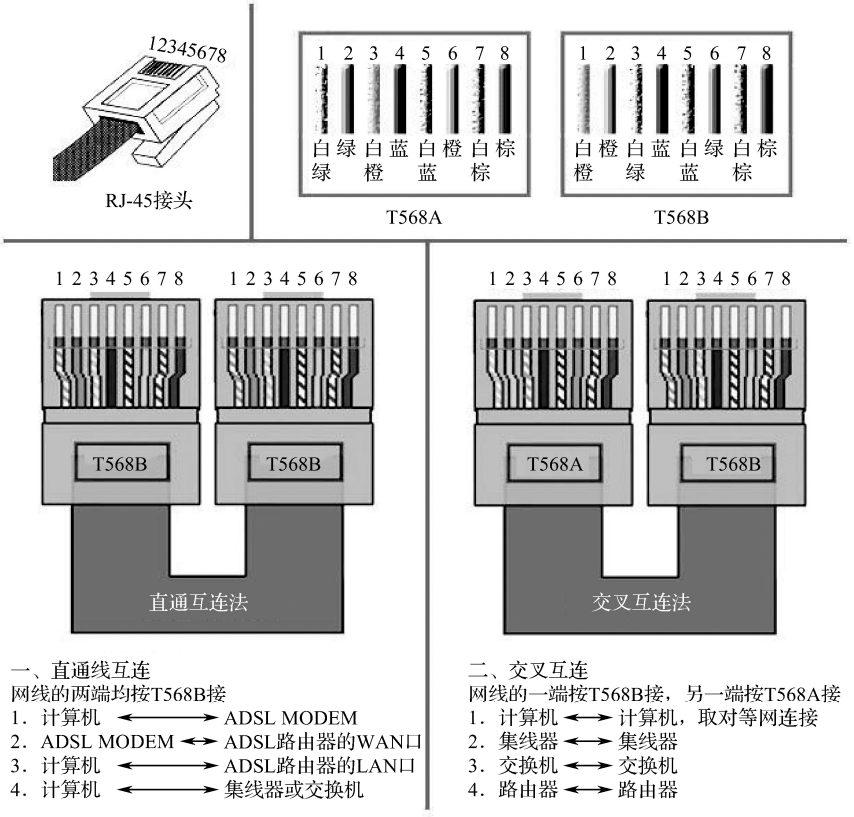


图 3-29　双绞线及其连接方法对比

4．双绞线插头的制作

双绞线插头的制作过程可简单归纳为“剥”、“理”、“插”、“压”四个字，按交叉线接法制作一根双绞线一端插头的具体步骤如下。

步骤 1：准备好 5 类双绞线、RJ45 插头和一把专用的压线钳。

步骤 2：用压线钳的剥线刀口将 5 类双绞线的外保护套管划开（小心不要将里面双绞线的绝缘层划破），刀口距 5 类双绞线的端头至少 2cm。

步骤 3：将划开的外保护套管剥去（旋转、向外抽）。

步骤 4：露出 5 类线电缆中的 4 对双绞线。

步骤 5：按照 T568B 标准（白橙、橙、白绿、蓝、白蓝、绿、白棕、棕）和导线颜色将导线按规定的序号排好。

步骤 6：将 8 根导线平坦、整齐地平行排列，导线间不留空隙。

步骤 7：准备用压线钳的剪线刀口将 8 根导线剪断。

步骤 8：剪断电缆线。请注意：一定要剪得很整齐。剥开的导线长度不可太短。可以先留

长一些。不要剥开每根导线的绝缘外层。

步骤 9：将剪断的电缆线放入 RJ45 插头试试长短（要插到底），电缆线的外保护层最后应能够在 RJ45 插头内的凹陷处被压实。反复调整。

步骤 10：在确认一切都正确后（特别要注意不要将导线的顺序排列反），将 RJ45 插头放入压线钳的压头槽内，准备最后的压实。

步骤 11：双手紧握压线钳的手柄，用力压紧。请注意，在这一步骤完成后，插头的 8 个引脚接触点就穿过导线的绝缘外层，分别和 8 根导线紧紧地压接在一起。

步骤 12：根据应用需求，制作双绞线的另一端插头。

双绞线制作完成后，可以用测试仪进行正确性测试，测试仪分为主测试仪和远程测试仪两部分（如图 3-30 所示）。首先将双绞线两端的插头分别插入主测试仪端和远程测试仪端的 RJ45 接口，然后观察测试仪两端指示灯亮的顺序是否与接线标准对应。

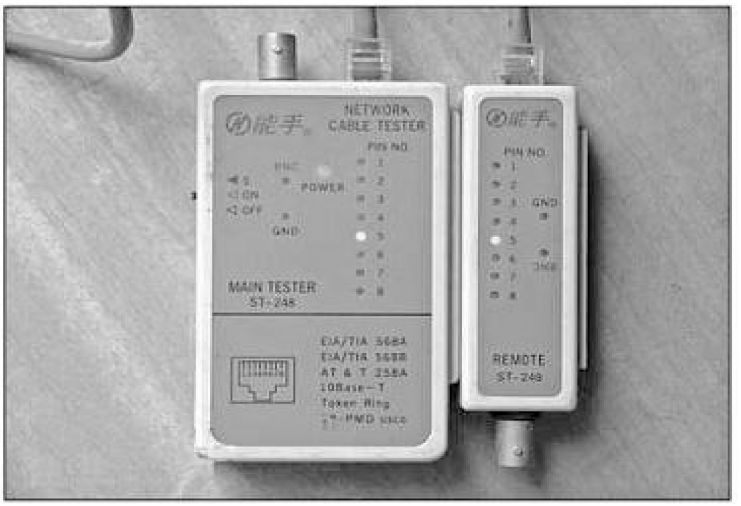


图 3-30　双绞线测试仪

如果线缆为交叉线缆，则其中一侧同样依次闪烁，而另一侧则会按 3、6、1、4、5、2、7、8 的顺序闪烁。如果测试的线缆为直连线缆，则测试仪上的 8 个指示灯应该依次闪烁。如果芯线顺序一样，但测试仪显示红色灯或黄色灯，则表明其中存在对应芯线接触不好的情况。此时就需要重做水晶头。

3.4.3　光纤

光纤通信现在在局域网和广域网中都有普遍应用。它以激光作为信息载体，以光导纤维（光纤）作为信息传递的传输介质。

光纤通信的优点：一是传输频带宽，数据传输速率高。可见光的频率在 1014～1015Hz 之间，能以 2Gbps 的数据速率传输几十千米。因此，一根光缆上能很容易地传输几十万路电话和几十路电视节目。光纤通信的通信容量是微波通信的 10 万倍；二是光纤传输损耗低，无中继传输距离远，适合于长距离传输应用。目前，以硅玻璃为基质材料的光纤无中继通信距离可达 100km 以上，几乎所有地面和海底的干线传输都采用光缆；三是光纤体积小、重量轻、可绕性

强，便于运输和敷设。同等传输速率的情况下，光缆比同轴电缆或双绞线轻便小巧很多；四是光纤是绝缘材料，传输的是光信号，完全实现电气隔离，能抗电磁干扰，防闪电雷击，也不会对其他系统产生电磁辐射；五是几乎无信号泄漏和串音，安全可靠，保密性强；六是光纤是玻璃制品，耐腐蚀，抗酸碱；七是节省能源；八是原料资源丰富。

光纤安装的工艺和设备要求很高，如果连接处不精确就会造成较大的信号衰减，这也使得光纤很难随意从中间抽头，只能用于点到点连接，但也带来保密性好这一优点。

光纤是典型的数字信道。光纤中传输的二进制数字“0”和“1”是怎么定义的呢？人们用光脉冲的出现表示“1”，不出现则表示“0”。它由二进制数字信号对光源进行通断调制而产生。因光纤通信的数据传输速率高（可达几千兆位每秒），传输距离远（无中继传输距离达几十千米甚至上百千米），而且不会向外界辐射电子信号，所以使用光纤介质的网络无论是在安全性、可靠性，还是网络性能方面都有了很大的提高，因而被广泛应用于军事网络通信中。

1．光纤的结构

光纤是光导纤维的简称，是一种细如头发丝的透明玻璃丝。它透明、纤细，虽比头发丝还细，却具有把光封闭在其中并沿轴向传播的导波结构。其结构和同轴电缆相似，也是呈圆柱形，只是没有网状金属屏蔽层，如图 3-31 所示。光纤由内向外有玻璃内芯、玻璃封套和塑料外套三层。

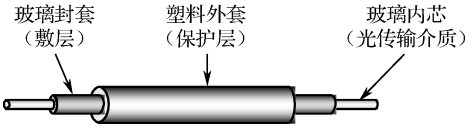


图 3-31　光纤结构示意图

纤芯位于光纤的中心部位，是以高纯度的二氧化硅为主要成分的石英玻璃丝，是光纤传输光信号的主要部分。光纤的线芯直径一般都被设计为 8～50μm。敷层也称为包层，位于纤芯的周围，是一层折射率比纤芯低的玻璃封套，其主要功能是防止光信号的泄漏。内部敷层的直径约为 125μm。塑料保护层的主要作用是增加光纤的机械强度和可弯曲性，以保护光纤的内部免遭损坏。

2．光纤的导光原理

光纤为什么会像金属导线那样能够传输信号呢？光在光纤中传输利用了光的全反射原理。纤芯的折射率比内部敷层的折射率稍微大一些。它满足光学原理中全反射的一个条件。由光发送机射入纤芯端面上的光也并非全部进入光纤，其中的一部分从光纤端面反射掉了。进入纤芯后的光将沿直线继续传播，直到射到纤芯与内部敷层的交界面上。

只要满足光学原理中全反射的另一个条件（光的入射角大于临界角），光就会在纤芯内发生全反射，全部由交界面偏向中心。当光碰到对面的交界面时，又全反射回来。光纤中的光就是这样在纤芯和敷层交界面上不断地发生全反射，从而从光纤的一端传向远方的另一端，而不会漏射到敷层中去。

光在传播过程中产生全反射的两个必备条件之一：光必须从折射率高的介质射入折射率低的介质，或者光的入射角大于临界角。

纤芯比包层的折射率高。当光线从高折射率的介质射向低折射率的介质时，其折射角将大

于入射角。因此，如果入射角足够大，就会出现全反射，即光线碰到包层时就会折射回纤芯。这个过程不断重复，光也就沿着光纤传输下去。如图 3-32 所示，光纤中的光就是这样在纤芯和包层交界面上不断地来回全反射的。

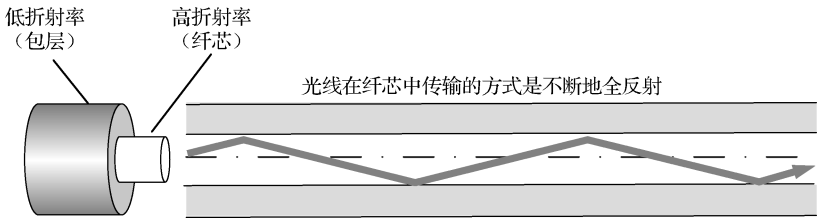


图 3-32　光在光纤中的传播示意图

因此，进入光纤中的光必须以一定的角度范围入射。如果超过此范围，则会有一部分光线进入敷层，从而跑到纤芯外面去了。那么，当光纤弯曲时，光线是否还能沿光纤传播呢？回答是肯定的。当光纤拐弯时，只要弯曲不是十分厉害，光也不会折射到敷层中去，仍然会全反射回来，只是来回反射的次数增多了。弯曲给光纤带来的光能损耗是很小的，可以忽略不计。

3．光纤的传输模式

（1）多模光纤

在给定的工作波长下可以有多个模式的光同时在光纤中传输，这种光纤称为多模光纤。多模光纤的纤芯直径为 50～62.5μm，包层外直径为 125μm，大致与人的头发粗细相当。它采用发光二极管作为光源，定向性较差。当光纤芯线的直径比光波波长大很多时，由于光束进入芯线中的角度不同，传播路径也不同，这时光束是以多种模式在芯线内不断反射而向前传播的，如图 3-33（a）所示。

多模光纤使用的光波长为 850nm 或 1300nm。在给定的工作波长下，多模光纤可以在单根光纤上同时传输几种光波，因而形成模分散，限制了带宽和距离。其中，能容纳多条满足全反射条件的光线同时在光纤中传输，光线以波浪式前进的多模光纤称为多模突变光纤；而每条入射光线的折射率不同，光线以抛物线式前进的多模光纤称为多模渐变光纤。

与单模光纤相比，多模光纤芯线粗，传输速度低、距离短（一般在 2km 以内），但其成本低。一般用于建筑物内或地理位置相邻的环境下。

（2）单模光纤

单模光纤的纤芯直径为 8.3μm，包层外直径为 125μm，仅有一条光通路，采用固体激光器作为光源。激光的定向性强，不会产生多次反射光线，而只沿光纤的内芯一直向前传播，如图 3-33（b）所示。目前在有线电视和光通信中，单模光纤是应用最广泛的。

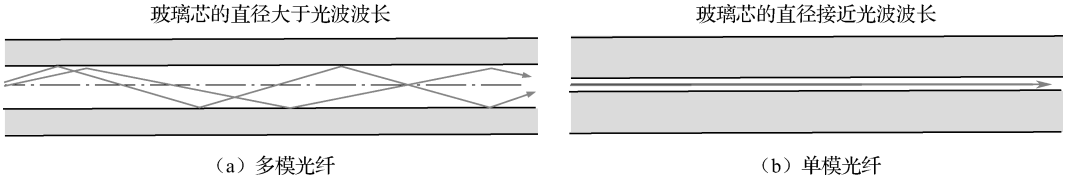


图 3-33　光纤传播模式

单模光纤使用的光波长为 1310nm 或 1550nm。单模光纤在给定的工作波长上只允许一束

光传播，没有模分散特性，离散很小，光信号损耗也很低，使得单模光纤的传输频带宽，传输带宽可达 3～50GHz/km，传播距离在 2km 以上，因而适用于大容量、长距离的光纤通信。

与多模光纤相比，单模光纤能高速传输更远的距离而不需要中继，而且传输速度快，但是光纤成本较高。

4．光缆

在实际应用中多使用光缆而不是光纤。因为一根光纤只能单向传输数据，所以在连接两个设备时至少需要两根光纤，一根用于发送数据，另一根用于接收数据。

光缆是由一组光纤组成的，也就是说，将若干根光纤捆绑在一起即是光缆。根据光纤的数量不同，可以分为单芯光缆、双芯光缆，甚至还有 12 芯、24 芯、48 芯、1000 芯等。为了便于安装和维护，一般还要在组成一根光缆的多对光纤外面包裹一层外护套，用于防潮、防擦伤、防压伤等，并在外护套内放置一些填充物。另外，室外光缆中还有一根加强钢丝，以增强光缆的整体抗拉性能，便于室外架设。图 3-34 所示是室外四芯光缆截面示意图。

光缆可以依所使用的光纤的模式来分类，分为单模光缆、多模光缆；也可以依据光缆中所含的光纤数目来分类，分为单芯光缆、双芯光缆、12 芯光缆、24 芯光缆等；还可以针对应用和环境条件的不同进行分类，分为室内光缆和室外光缆。室内光缆主要用于室内布线。室内光缆多为紧套结构，具有柔软、方便插接、阻燃等优点。室外光缆用于建筑群间布线或远程通信或干线布线。一般都用金属皮包裹，具有抗拉伸、抗侧压、防水性能好等特点。

5．光纤跳线

光纤跳线是指光纤两端都装上连接器插头、用于与桌面计算机或设备直接相连的光纤，以方便设备的连接和管理。光纤跳线由光纤、接头两部分组成，如图 3-35 所示。

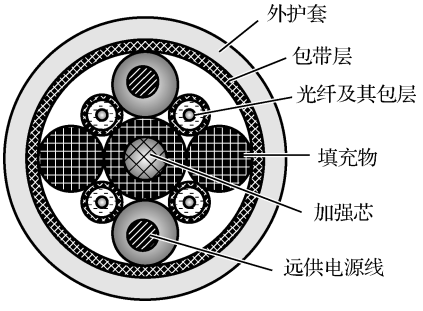


图 3-34　室外四芯光缆截面示意图

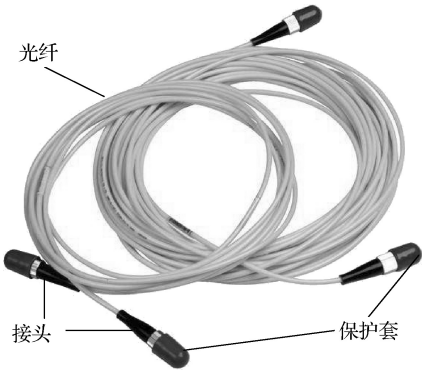


图 3-35　光纤跳线的组成

根据传输介质的不同，光纤跳线可分为单模跳线和多模跳线两类，分别与单模光纤和多模光纤连接。单模光纤跳线的光纤部分一般为黄色保护层，接头和保护套为蓝色，传输距离较长。多模光纤跳线的光纤部分一般为橙色保护层，也有用灰色的，接头和保护套用米色或黑色，传输距离较短。

在使用光纤跳线时，一定要注意区分跳线的形式，尤其是颜色。因为光纤跳线两端的光模块的收发波长必须一致，也就是说光纤的两端必须是相同波长的光模块。简单的区分方法是跳线的颜色和光模块的颜色要一致。一般情况下，短波光模块使用多模光纤（橙色），长波光模

块使用单模光纤（黄色），这样才能保证数据传输的正确性。此外，光纤在使用中不要过度弯曲和绕环，否则会增加光在传输过程的衰减。使用光纤跳线后，一定要用保护套将光纤接头保护起来，灰尘和油污将会损害光纤的耦合。

光纤跳线的制作较困难、技术要求较高。因此，光纤跳线是由专业厂家的专业人员使用专门设备生产出来的。普通用户可向生产厂家或网络公司等定制、购买。按接头结构的不同，光纤跳线可分为 FC、SC、ST 等常见形式，如图 3-36 所示。

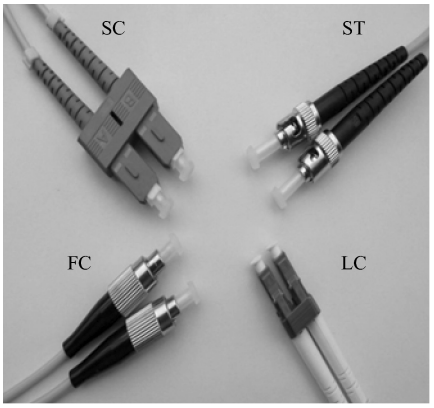


图 3-36　光纤跳线接头

6．光纤连接器

在安装任何光纤系统时都必须考虑以低损耗的方法把光纤或光缆相互连接起来，以实现光链路的接续。光纤链路的接续可以分为永久性的和活动性的两种。永久性接续，大多采用熔接法、粘接法或固定连接器来实现；活动性接续，一般采用活动连接器来实现。永久性连接一般由专业网络公司完成。因此，这里仅介绍活动连接器。

光纤活动连接器一般称为光纤连接器，俗称活接头，是用于连接两根光纤或光缆形成连续光通路的可以重复使用的无源器件，已经广泛应用在光纤传输线路、光纤配线架和光纤测试仪器及仪表中。

按照不同的分类方法，光纤连接器有不同的种类：按传输介质的不同可分为单模光纤连接器和多模光纤连接器；按结构的不同可分为 FC、SC、ST、D4、DIN、Biconic、MU、LC、MT 等各种形式的光纤连接器；按连接器的插针端面可分为 FC、PC（UPC）和 APC；按光纤芯数分还有单芯、多芯之分。以下简单介绍一些常见的光纤连接器。

（1）FC 型光纤连接器

这种连接器最早由日本 NTT 研制。FC 是 Ferrule Connector 的缩写，表明其外部加强方式是采用金属套，紧固方式为螺丝扣。此类连接器结构简单，操作方便，制作容易。

（2）SC 型光纤连接器

这也是由日本 NTT 公司开发的。其外壳呈矩形，所采用的插针和耦合套筒的结构尺寸与 FC 型完全相同，紧固方式采用插拔式，不需要旋转。此类连接器价格低廉，插拔操作方便，介入损耗波动小，抗压强度较高，目前使用最多。

（3）MT-RJ 型连接器

MT-RJ 起步于 NTT 开发的 MT 连接器，带有与 RJ45 型 LAN 电连接器相同的闩锁机构，通过安装于小型套管两侧的导向销对准光纤，为便于与光收发信机相连，连接器端面光纤为双

芯（间隔 0.75mm）排列设计，属于高密度光连接器。

（4）LC 型连接器

LC 型连接器是 Bell 研究所开发的，采用操作方便的模块化插孔（RJ）闩锁机理制成。其所采用的插针和套筒的尺寸是普通 SC、FC 等所用尺寸的一半，为 1.25mm，这样可以提高光配线架中光纤连接器的密度。

（5）MU 型连接器

MU（Miniature unit Coupling）连接器以 SC 型连接器为基础，是由 NTT 研制开发的世界上最小的单芯光纤连接器，其优势在于能实现高密度安装，适应光纤网络更大带宽、更大容量的发展方向。

使用光纤连接器的注意事项如下：

① 光纤连接器的插针要保持清洁，不使用时一定要戴好光纤保护帽。

② 光纤连接器的光纤部分禁止直角和锐角弯折，严禁受重物挤压，纤体有折痕、压痕、破损的连接器不能使用，纤体的盘绕半径需要大于 30mm。

③ 不要用眼直视已与光设备连接的光纤连接器端面，否则会对视力造成伤害。

④ 确认光连接器类型与光纤类型配套，并注意分清光纤接口的收发极性。

习题

1．简述以太网的概念及类型。
2．以太网有哪两个主要标准？
3．说明 10Base-T 中的“10”、“Base”和“T”所代表的含义。
4．简述以太网交换机的功能。
5．以太网交换机有何特点？它与集线器有何区别？
6．如何利用交换机进行 VLAN 划分？
7．PPP 的主要特点是什么？
8．什么是调制解调器的专线方式？有什么特点？
9．常用的传输介质有哪几种？各有何特点？
10．调制解调器有什么作用？
11．如何制作用于连接两台计算机的双绞线？
12．简述光纤的结构、原理、分类和通信特点。
13．说明 IP 地址与硬件地址的区别。为什么要使用这两种不同的地址？
14．E1 接口有哪几种使用方法？
15．接口转换器的功能有哪些？

Chapter 4

第4章

军事广域网络技术

【主要内容】 介绍 IP 连网技术、网络互连原理、广域网络技术及路由器有关知识。包括 IP 地址的类型、特点、与广域路由的关系和子网规划方法，路由器在网络互连中的关键作用、工作原理及其路由算法与典型协议，宽带 IP 网络及 ATM、SDH、DDN 等广域网络的技术特点，VPN 虚拟专用网技术和 MPLS 交换协议的工作原理与特点，路由器的选购、连接与配置等。

4.1 IP 连网技术

IP 协议可横跨局域网、广域网，几乎所有局域网、广域网系统及设备均支持 IP 协议，是不同介质传输方式的最佳协议。IP 为数据报类协议，其传输响应时间较好，协议交互少，较适合于数据高速传输的需要，目前广泛使用的是 IPv4 版，为了克服 IP 协议的一些不足，又发展了新的 IPv6 版。

4.1.1 分类的 IP 地址及其特点

IP 协议是 TCP/IP 协议族中网络层的协议，是 TCP/IP 协议族的核心协议，是现今不同硬件结构、不同操作系统、不同应用系统的计算机网络实现互联互通的基石性协议，可运行在各种各样的底层网络上，如端对端的串行数据链路（PPP 协议和 SLIP 协议）、以太网（Ether）、卫星链路等。通过 IP 协议实现各种异构网络互连，IP 地址发挥了重要作用。

在一个局域网中，如果不需要与外界网络进行通信，内部网络的各计算机都能识别其他节点，完全可以通过交换机实现数据传送，根本用不到路由器来记忆局域网的各节点 MAC 地址。路由器识别不同网络是通过识别不同网络的网络 ID 号进行的，所以为了保证路由成功，每个网络都必须有一个唯一的网络编号。网络传输的数据分组包含了 IP 信息，其中的 IP 地址则包含了网络编号信息。

1．IP 地址的结构

每个 IP 地址都包含网络 ID 和主机 ID 两部分。网络 ID 标识同一个物理网络上的所有宿主机，主机 ID 标识该物理网络上的每一个宿主机，于是整个网络上的每台计算机都依靠各自唯一的 IP 地址来标识。从网络的层次结构考虑，一个 IP 地址必须指明两点：一是某 IP 主机属于哪个网络；二是该 IP 主机到底是这个网络中的哪台主机。

IP 地址结构分两个等级的好处是：第一，IP 地址管理机构在分配 IP 地址时只分配网络地址，而剩下的主机号则由得到该网络地址的单位自行分配，这样就方便了 IP 地址的管理；第二，路由器仅根据目的主机所连接的网络地址来转发分组（而不考虑目的主机号），这样就可以使路由表中的项目数大幅减少，从而减小了路由表所占的存储空间。

IP 地址是标志一个主机（或路由器）和一条链路的接口。当一个主机同时连接到两个网络上时，该主机就必须同时具有两个相应的 IP 地址，其网络地址 net-id 必须是不同的。由于一个路由器至少应当连接到两个网络（这样它才能将 IP 数据报从一个网络转发到另一个网络），因此一个路由器至少应当有两个不同的 IP 地址。网络地址相同的网络，无论是范围很小的局域网，还是可能覆盖很大地理范围的广域网，都是平等的同一个网络。

总结起来，IP 地址具有如下特点。

（1）IP 地址不能反映任何有关主机位置的物理信息；

（2）一个主机同时连接在多个网络上时，该主机必须有多个 IP 地址；

（3）由集线器连接起来的若干个局域网仍为一个网络；

（4）所有分配到网络 ID 号的网络都是平等的；

（5）IP 地址可用来指明一个网络的地址。

IP 地址的编址方法有三类。一是分类的 IP 地址，这是最基本的编址方法，在 1981 年就通过了相应的标准协议。二是子网的划分，这是对最基本的编址方法的改进，其标准（RFC 950）在 1985 年通过。三是构成超网，这是比较新的无分类编址方法。1993 年提出后很快就得到推广应用。

2．分类的 IP 地址

目前使用 32 比特的 IPv4 地址，用 4 个点分十进制数表示，如 202.112.14.1。它主要由两部分组成：一部分是用于标识所属网络的网络地址；另一部分用于标识给定网络上某个特定的主机地址。这种编址方法将 IP 地址空间划分为几个不同的地址类别，以适应不同规模的网络。

分类的 IP 地址表示法将所有 IP 地址分成 A、B、C、D、E 五类。每一类地址都由两个固定长度的字段组成，其中一个字段是网络地址（net-id），它标识主机（或路由器）所连接到的网络，而另一个字段则是主机号（host-id），它标识该主机（或路由器）。

（1）A 类地址

A 类地址第 1 字节为网络地址，前面 1 位为类别位，数值为 0，余下 7 比特为网络地址，

其他 3 字节为主机地址。A 类地址允许有（2^7–2）即 126 个网络，每个网络允许有（2^{24}–2）即 1670 万台主机，通常分配给拥有大量主机的网络（如主干网）。

（2）B 类地址

B 类地址第 1 字节和第 2 字节为网络地址，前面 2 位为类别位，数值为 10，余下 14 位为网络地址，其他 2 字节为主机地址。B 类地址允许有（2^{14}–1）即 16 384 个网络，每个网络允许有（2^{16}–2）即 65 533 台主机，适用于节点比较多的网络。

（3）C 类地址

C 类地址第 1 字节、第 2 字节和第 3 个字节为网络地址，前面 3 位为类别位，数值为 110。第 4 字节为主机地址。C 类地址允许有（2^{21}–1）个网络，每个网络允许有（2^8–2）即 254 台主机，适用于节点比较少的网络。

（4）D 类地址

D 类地址的范围及含义如表 4-1 所示。D 类地址不分网络地址和主机地址，它的第 1 字节的前四位固定为 1110，D 类地址表示一个多播地址，即多目的地传输，可用来识别一组主机，多用于一些特定的程序及多媒体程序。D 类地址不能出现在 IP 报文的源 IP 地址字段。

表 4-1　D 类地址的范围及含义

D 类地址范围	含　义
224.0.0.0～224.0.0.255	预留的组播地址（永久组地址），地址 224.0.0.0 保留不做分配，其他地址供路由协议使用
224.0.1.0～238.255.255.255	用户可用的组播地址（临时组地址），全网范围内有效
239.0.0.0～239.255.255.255	本地管理组播地址，仅在特定的本地范围内有效

224.0.0.1 特指本网络的所有主机，224.0.0.2 特指本网络的所有组播路由器。D 类地址是动态分配的，组播结束即回收。IETF 建议本地站点组播选用 239.253.0.0～239.253.0.16 范围的地址，在本地机构内组播选用 239.192.0.0～239.192.0.14 范围的地址。

（5）E 类地址

E 类地址也不分网络地址和主机地址，它的第 1 字节的前五位固定为 11110，暂未使用。

各类型 IP 地址的范围及其保留地址和私有地址如表 4-2 所示。

表 4-2　各类型 IP 地址的范围及其保留地址和私有地址

类　型	IP 地址范围	保留 IP	私有 IP
A 类	1.0.0.1～126.255.255.254	127.X.X.X	10.0.0.0-10.255.255.255
B 类	128.0.0.1～191.255.255.254	128.0.X.X	172.16.0.0—172.31.255.255
C 类	192.0.0.1～223.255.255.254		192.168.0.0-192.168.255.255
D 类	224.0.0.1～239.255.255.254		
E 类	240.0.0.1～255.255.255.254		

3．特殊的 IP 地址

（1）私有地址

上面提到 IP 地址在全世界范围内唯一，但像 192.168.0.1 这样的地址在许多地方都能看到，并不唯一，这是为何？Internet 管理委员会规定 10.0.0.0～10.255.255.255、172.16.0.0～

172.131.255.255、192.168.0.0～192.168.255.255 地址段为私有地址。私有地址可以在内部组网时使用，使得能连通内部主机，而不能连通外网主机，既可以申请较少的外网地址，还有利于保证内网的安全。

私有地址被大量用于单位内部局域网络中。一些宽带路由器也往往使用 192.168.X.1 作为默认地址。私有网络由于不与外部互连，因而可能使用随意的 IP 地址。保留这样的地址是为了避免以后接入公网时引起地址混乱。在互联网上，私有地址是不能出现的，出口路由器也没有这些地址的路由。使用私有地址的私有网络在接入互联网时，要使用具有网络地址转换（NAT）功能的路由器或代理服务器，将私有地址翻译成公用合法地址。

NAT 一般以软件形式存在于路由器中，并可以配置成静态地址转换、动态地址转换、复用动态地址转换等形式，既可用于对私有地址进行转换，也可用于一般的内部地址转换。静态地址转换将内部本地地址与公用合法地址进行一对一的转换。如果内部网络有 E-mail 服务器或 FTP 服务器等可以为外部用户共用的服务，则这些服务器的 IP 地址必须采用静态地址转换，以便外部用户可以使用这些服务。动态地址转换从公用合法地址池中动态地选择一个未使用的地址对内部本地地址进行转换。复用动态地址转换首先是一种动态地址转换，但是它可以允许多个内部本地地址共用一个公用合法地址，在公用合法地址个数较少时极为有用。

（2）保留地址

A 类网络地址 127.X.X.X 是一个保留地址，用于网络软件测试及本地机进程间通信，也叫作回送地址（loopback address）。无论什么程序，一旦使用回送地址发送数据，协议软件立即返回之，主机和网关不转发该地址。含网络地址 127 的分组不能出现在任何网络上。

因此，ping 127.0.0.1 如果反馈信息失败，说明 IP 协议栈有错，必须重新安装 TCP/IP 协议。如果 ping 本机 IP 地址，反馈信息失败，说明网卡不能和 IP 协议栈进行通信。如果网卡没接网线，用本机的一些服务（如 SQL Server、IIS 等）就可以使用 127.0.0.1 这个地址。

128.0.X.X 作为保留地址，不指派。B 类的 169.254.X.X 也是保留地址。如果 IP 地址是自动获取 IP 地址，而网络上又没有找到可用的 DHCP 服务器，Windows 系统会自动分配这样一个地址。如果发现主机 IP 地址是一个诸如此类的地址，这时可能 DHCP 服务器或网络发生了故障。

（3）广播地址

TCP/IP 规定，主机号全为“1”的网络地址或 32 比特全为“1”（即 255.255.255.255）用于广播，叫作广播地址。所谓广播，指同时向同一子网所有主机发送报文。如果主机向其他网络的所有节点广播信息，即直接广播，可以用一个有效的网络地址和一个全“1”的主机号，如 202.93.120.255，发送直接广播前需要知道目的网络的网络地址。若主机试图在本网内通信而又不知道本网网络地址，可以利用 0 地址，这也称有限广播，即广播被限制在本子网之中，IP 构成如 255.255.255.255，发送有限广播前不需要知道网络地址。

（4）网络地址

TCP/IP 协议规定，主机地址全为“0”或各位全为“0”的网络地址被解释成“本”网络，常用在路由表中。

对一台网络上的主机来说，它可以正常接收的合法目的网络地址有三种：本机的 IP 地址、广播地址及组播地址。

4.1.2 子网划分

为了克服 IP 地址的浪费现象、提高 IP 地址的使用效率及路由效率，在基础的 IP 地址分类上对 IP 编址进行了相应的改进。

1．子网划分方法

子网划分问题的提出原因主要是克服 IP 地址分配不合理、利用率低的问题，使 IP 地址能适应不同的网络规模。为提高 IP 地址的使用效率，1985 年 RFC 950 提出了子网划分方法，对最基本的编址方法进行了改进。

子网划分方法：将 IP 地址的主机号部分进一步划分成子网部分和主机部分，从标准 IP 地址的主机号部分“借”位并把它们指定为子网号部分，在“借”用时必须给主机号部分剩余 2 位，在“借”用时至少要借用 2 位。形成这种模式：网络地址+子网号+主机号，如图 4-1 所示。

图 4-1　子网编址的层次结构

在原来的 IP 地址模式中，网络地址部分就标识一个独立的物理网络。引入子网模式后，网络地址部分加上子网号才能全局唯一地标识一个物理网络。子网编址使得 IP 地址具有一定的内部层次结构，这种层次结构便于 IP 地址分配和管理。它的使用关键在于选择合适的层次结构——如何既能适应各种现实的物理网络规模，又能充分地利用 IP 地址空间，即从何处分隔子网号和主机号。

2．子网掩码与网关

为了反映 IP 地址位中有多少位用于子网号，采用子网掩码来区分。二进制表示的掩码是一系列连续的“1”，紧跟着一系列连续的“0”。为“1”的部分代表网络地址码，而为“0”的部分代表主机号码。以 10.0.0.1 为例，网络掩码 255.0.0.0，这样就把 IP 地址分成了网络部分 10 和主机部分 0.0.1。于是，每个 A、B 和 C 类地址都有一个默认子网掩码，A 类：255.0.0.0；B 类：255.255.0.0；C 类：255.255.255.0。

在子网编址模式下，仅凭地址类别提取地址的网络地址和主机号将是不正确的，必须在路由表的每一个表目中加入子网掩码，于是子网编址模式下的路由表条目变为：{目的网络地址，子网掩码，下一路由器地址}，这样可以用子网掩码的设置来区分不同的情况，使路由算法更简单。

子网掩码只有一个作用，就是将某个 IP 地址划分成网络地址和主机地址两部分。因此，子网掩码不能单独存在，必须结合 IP 地址一起使用，路由器网络据其“计算”出某个 IP 的网络地址，以便于数据转发。计算机要在同一网络（也就是说它们的网络地址必须相同，而且主机地址必须不一样），才能通过网线直接连接或者通过 HUB 或普通交换机间接进行数据传输。

如果两个主机不在一个网络，就需要网关进行路径选择。主机网卡或其所在网络的网关通

过子网掩码“计算”得到 IP 地址的网络地址，就是判断该 IP 主机所在的子网是本网还是其他子网。这里的网关是一个概念，是指在传输层以上实现广域网络互连或局域网络互连的设备。网关实现对不同网络体系结构、通信协议、数据格式的两个网络的“翻译”，通过协议转换、路由选择、重新打包、数据交换等步骤将一个网络的数据转发到另一个网络，因此又被称作网间连接器、协议转换器。具体设备可以是一个路由器、三层交换机、防火墙或启用了路由功能的计算机服务器。一般地，路由器的 LAN 接口的 IP 地址就是本地局域网的网关。

例如，当主机 A 要把数据传送给主机 B 时，主机 A 先通过自己主机的子网掩码计算出主机 A 的网络 ID；然后，再利用主机 B 的 IP 地址和自己的子网掩码，计算出主机 B 的网络 ID。如果自己和主机 B 的网络 ID 相同，说明在一个网段，则直接传送；否则，说明主机 A 和 B 不在同一个网段，即使它们通过交换机（或集线器）物理连接，也不能相互通信，这时就需要通过路由器或启用了路由协议的（代理）服务器（即 TCP/IP 协议配置中所指定的本网络的“默认网关”）来转发数据包。主机 A 把数据包发给网关 A，再由网关 A 通过路由选择后转发到主机 B 所在的网关 B，由网关 B 将数据包最终转发给主机 B。因此，只有设置好网关的 IP 地址，TCP/IP 才能实现不同网络之间的相互通信。一台主机可以有多个网关，当其找不到可用网关时，就把数据包发给用户指定的“默认网关”。

从上可见，通过子网掩码“计算”网络地址对于分组转发非常重要。网络地址的计算方法：子网号=子网掩码与 IP 地址做逻辑“与”运算的结果。实际上，还可由此得到该网络的广播地址、地址范围及本网有几台主机等信息。

例 4-1：主机 IP 地址为 192.168.100.5，子网掩码是 255.255.255.0。其网络地址、广播地址、地址范围、主机数的计算方法如下：

（1）将 IP 地址和子网掩码换算为二进制，子网掩码连续全 1 的是网络地址，后面的是主机地址。

192.168.100.5　　11000000.10101000.01100100.00000101
255.255.255.0　　11111111.11111111.11111111.00000000

（2）IP 地址和子网掩码进行“与”运算，结果是网络地址。

将 IP 地址和子网掩码都换算成上述的二进制，然后进行逐位“与”运算，结果就是网络地址。1 与 1 相“与”等于 1，1 与 0 相“与”等于 0，0 与 0 相“与”等于 0。

网络地址的计算结果为：192.168.100.0，即 11000000.10101000.01100100.00000000。

（3）上面的网络地址中的网络地址部分不变，主机地址变为全 1，结果就是广播地址：192.168.100.255，即 11000000.10101000.01100100.11111111。

（4）地址范围就是含在本网段内的所有主机

网络地址加 1 即为第一个主机地址，广播地址减 1 即为最后一个主机地址，由此可以看出本例的网络范围是：192.168.100.1～192.168.100.254。

也就是说这些地址都是一个网段的：

192.168.100.1
192.168.100.2
192.168.100.20
192.168.100.111
⋮
192.168.100.254

（5）主机的数量

假设主机所占位数为 n 比特，主机的数量 $m=2^n-2$。减 2 是因为主机不包括网络地址和广播地址。本例二进制的主机位数是 8 位。所以主机数量为：$2^8-2=254$。

例 4-2：某单位分配到一个 B 类 IP 地址，其 net-id 为 129.250.0.0。该单位有 4000 台机器，平均分布在 16 个不同的地点。如果选用子网掩码为 255.255.255.0，试给每一地点分配一个子网号码，并计算出每个地点主机号码的最小值和最大值。

（1）子网数量和子网主机数量确定。总的主机数量为 4000 台，子网数量为 16，平均每个子网的主机数量为 4000/16=250，平均每个地点 250 台机器。

（2）如选 255.255.255.0 为掩码，则每个网络所连主机数=$2^8-2=254>250$，子网总数=$2^8-2=254>16$，子网号选用低的 5 位即能满足实际需求。

（3）可给每个地点分配如下子网号码：

地点	子网号	子网网络地址	主机 IP 的最小值	主机 IP 的最大值
1	00000001	129.250.1.0	129.250.1.1	129.250.1.254
2	00000010	129.250.2.0	129.250.2.1	129.250.2.254
3	00000111	129.250.3.0	129.250.3.1	129.250.3.254
⋮	⋮	⋮	⋮	⋮
15	00001111	129.250.15.0	129.250.15.1	129.250.15.254
16	00010000	129.250.16.0	129.250.16.1	129.250.16.254

4.1.3 CIDR 无类别编址

1．VLSM 可变长子网掩码

VLSM（Variable Length Subnet Mask，变长子网掩码）是一种产生不同大小子网的网络分配机制，指一个网络可以配置不同的掩码。开发可变长度子网掩码的想法就是在每个子网上保留足够的主机数的同时，把一个网分成多个子网时有更大的灵活性。如果没有 VLSM，一个子网掩码只能提供给一个网络，这样就限制了要求的子网数上的主机数。

VLSM 技术对高效分配 IP 地址（较少浪费）及减少路由表大小都起到非常重要的作用，但是需要注意的是使用 VLSM 时，所采用的路由协议必须能够支持它，这些路由协议包括 RIP2、OSPF、EIGRP 和 BGP。

2．CIDR 无类别编址方法

为限制 Internet 主干路由器中必要路由信息的增长，引入了无类域间路由（Classless Inter-Domain Routing，CIDR），它意味着在路由表层次的网络地址“类”的概念已经被取消，代之以“网络前缀”的概念。

CIDR 的基本思想是忽略 A、B、C 三类地址之间的差别及它们的网络地址和主机号之间的界线，代之的是允许以可变长分界的方式分配网络数，当给某个网络分配 IP 地址时，总是同时给出 32 位的网络地址和相应的 32 位地址掩码，掩码中值为 1 的位涵盖网络地址（网络地址），掩码中值为 0 的位涵盖主机地址。

CIDR 消除了传统的 A 类、B 类和 C 类地址及划分子网的概念，使用各种长度的“网络前

缀”（network-prefix）来代替分类地址中的网络地址和子网号，使得 IP 地址从使用子网掩码的三级编址又回到了两级编址。

CIDR 地址块的表示方法如 210.31.224.0/21，这个地址块的主机号是 11 位，斜线后的数字就是掩码中 1 的个数，子网掩码为 255.255.248.0。这个地址块的起始地址是 210.31.224.0，最小地址是 210.31.224.1，最大地址是 210.31.231.254。

CIDR 地址记法的其他形式为 10.0.0.0/10，可简写为 10/10，也就是把点分十进制中低位连续的 0 省略；也可在网络前缀的后面加一个星号，如 00001010 00*，在星号“*”之前是网络前缀，而星号“*”表示 IP 地址中的主机号。

CIDR 可以汇总 IP 地址，构成超网。在未作地址汇总之前，路由器需要对外声明所有的内部网络 IP 地址空间段。这将导致网络中的核心路由器的路由条目非常庞大。采用 CIDR 地址汇总后，可以将连续的地址空间块归结成一条路由条目。路由器不再需要对外声明内部网络的所有 IP 地址空间段。这样，就大大减少了路由表中路由条目的数量。这种地址的聚合常称为路由聚合，它使得路由表中的一个项目可以表示很多个传统分类地址的路由。

在图 4-2 所示的 CIDR 地址划分方法中，网络服务提供商 ISP 共有 64 个 C 类网络。如果不采用 CIDR 技术，则在与该 ISP 的路由器交换路由信息的每一个路由器的路由表中，就需要有 64 个项。但采用地址聚合后，只需用路由聚合后的 1 个项 206.0.64.0/18 就能找到该 ISP。

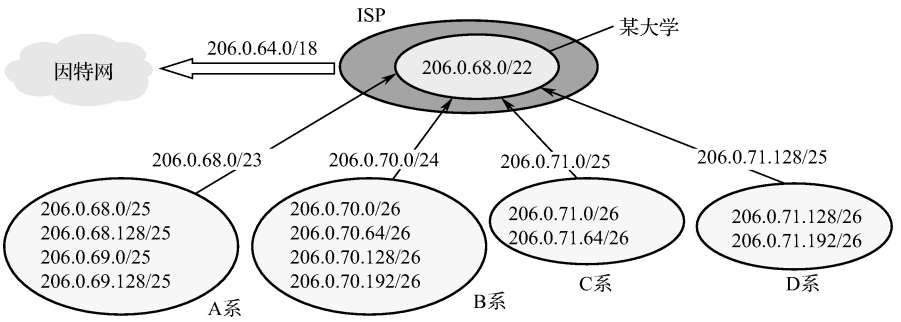


图 4-2　CIDR 地址划分方法

使用 CIDR 时，路由表中的每个项目都由“网络前缀”和“下一跳地址”组成。在查找路由表时可能会得到不止一个匹配结果，应当从匹配结果中选择具有最长网络前缀的路由——最长前缀匹配（longest-prefix matching）。网络前缀越长，其地址块就越小，因而路由就越具体。最长前缀匹配又称为最长匹配或最佳匹配。

例如，如果收到的分组的目的地址是 206.0.71.128，它与路由表中的项目 206.0.68.0/22（ISP）和 206.0.71.128/25（D 系）都能匹配，但 206.0.68.0/22 的掩码有 22 个连续的 1，而 206.0.71.128/25 的掩码有 25 个连续的 1，所以将分组转发到最长前缀的 D 系的路由器。

3．子网规划方法

在子网划分的 IP 编址方法和 CIDR 无类别编址方法中，某个网络或子网络的网络地址都是通过子网掩码（地址掩码）“计算”得到的。并且，子网掩码与 IP 地址结合使用，可以确定该 IP 地址所在的网络地址及该网络的地址范围和主机数量。因此，反过来，要将一定数量的主机划分成一个子网，则需为其定义合适的子网掩码。子网规划一般有两种情况：一是将一个网络地址已知的网络划分为若干个小的子网；二是设计一个新的网络，根据主机数目确定主网

络地址。

对一个网络进行子网规划，关键就是根据网络设备和主机所需 IP 地址的数量确定各个子网的子网掩码。其中，数量应去除网络地址、网络广播地址、子网地址、子网广播地址，因为按 TCP/IP 协议规定，这些地址都不能分配给任何设备或主机。还需特别注意的是，进行子网互连的路由器也需要占用有效的 IP 地址，在计算所需 IP 数量时，不要忘记连接该网络（或子网）的路由器应分配的 IP 地址。

子网规划的依据就是子网个数与占用主机地址位数满足等式：$n=2^m$。其中，m 表示占用主机地址的位数；n 表示划分的子网个数。子网规划就是根据子网个数要求及每一个子网的有效主机地址个数要求，确定借几位主机号作为子网号，然后写出借位后的子网个数、每一个子网的有效主机地址个数、每一个子网的子网地址、子网掩码和每一个子网的有效主机地址。

这样，定义子网掩码的步骤就是：

（1）将要划分的子网数目转换为 2 的 m 次方。如要分 8 个子网，$8=2^3$，即 $m=3$。

（2）将上一步确定的 m 按高序占用主机地址 m 位后转换为十进制。如 m 为 3，则是 11100000，转换为十进制为 224，即为最终确定的子网掩码。如果是 C 类网，则子网掩码为 255.255.255.224；如果是 B 类网，则子网掩码为 255.255.224.0；如果是 A 类网，则子网掩码为 255.224.0.0。

子网规划和 IP 地址分配在网络规划中占有重要地位。在确定借几位主机号作为子网号时应使子网号部分产生足够的子网，而剩余的主机号部分能容纳足够的主机。下面举例说明。

例 4-3：某军事网络系统由 4 个办公单位组成，假设每个单位所需计算机 25 台，给定该局域网络地址空间为 192.168.10.0，问如何给每个单位的子网分配 IP 号码段和子网掩码。

分析：192.168.10.0 是一个 C 类 IP 地址，标准掩码为 255.255.255.0，它们的表示形式如图 4-3 表示。

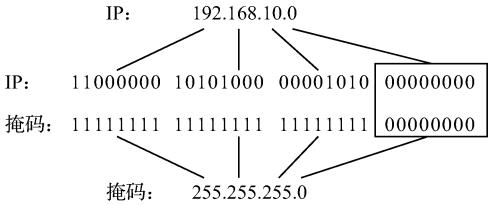


图 4-3 IP 地址及标准子网掩码表示形式

要划分为 4 个子网，必然要向后面的 8 位主机号借位，借几位呢？子网数为 4，需要借用 3 位，$2^3-2=6>4$，满足子网序号编号要求。8 位主机号借用 3 位后剩余 5 位，主机数量为 $2^5-2=30$，可以满足需求子网中主机编号要求。子网号借用情况如图 4-4 所示。

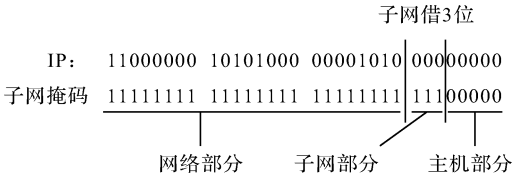


图 4-4 子网号与主机号的划分

确定了子网部分，后面就简单了，前面的网络部分不变，看最后的 8 位，如图 4-5 所示。

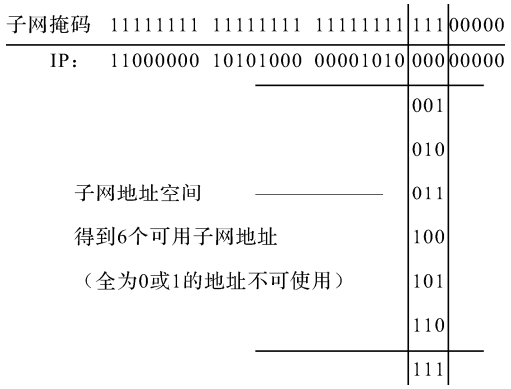


图 4-5　子网编址

与标准的 IP 地址相同，子网编址也为子网网络和子网广播保留了地址编号。因此，二进制全“0”或全“1”的子网号不能分配给实际的子网。在上面的例子中，二进制“000”和“111”所表示的子网号“0”和子网号“7”不能分配。由此得到 6 个可用的子网地址，用点分十进制表示如下：

11000000 10101000 00001010 00100000　　192.168.10.32/27
11000000 10101000 00001010 01000000　　192.168.10.64/27
11000000 10101000 00001010 01100000　　192.168.10.96/27
11000000 10101000 00001010 10000000　　192.168.10.128/27
11000000 10101000 00001010 10100000　　192.168.10.160/27
11000000 10101000 00001010 11000000　　192.168.10.192/27
子网掩码：11111111 11111111 11111111 11100000　　255.255.255.224

得出了所有子网的网络地址后，在对每个子网进行主机地址分配时也需注意有两个地址不可分配：主机地址全为 0 的 IP 是网络地址，全为 1 的 IP 是网络广播地址，所以每个子网的子网地址和主机地址如下。

子网 1：192.168.10.32/27，　掩码：255.255.255.224，　　主机 IP：192.168.10.33-62
子网 2：192.168.10.64/27，　掩码：255.255.255.224，　　主机 IP：192.168.10.65-94
子网 3：192.168.10.96/27，　掩码：255.255.255.224，　　主机 IP：192.168.10.97-126
子网 4：192.168.10.128/27，掩码：255.255.255.224，　　主机 IP：192.168.10.129-158
子网 5：192.168.10.160/27，掩码：255.255.255.224，　　主机 IP：192.168.10.161-190
子网 6：192.168.10.192/27，掩码：255.255.255.224，　　主机 IP：192.168.10.193-222

本例中，只要使用前面 4 个子网就可以了。

如果本案例中的局域网是新建设的，则需要在进行子网划分前规划并申请整个网络的网络地址。方法和划分子网时一样，通过公式计算（$2^m - 2 \geqslant n$），n 为最大主机数，得到子网位数 m。所以，如果要建设一个拥有 4 个子网、每个子网内有 25 台主机的网络，则“最大主机数”为(4+2)×(25+2)，即需 162 个 IP 地址。由于一个 C 类地址的网络可以拥有 254 个主机地址，所以可以选择 C 类地址作为整个网络的网络号。

CIDR 编址方法可以更为精细地根据需要分配 IP 地址，从而更有效地使用 IP 地址空间。基于 CIDR 的子网划分方法与上述类似。

4.1.4 IPv6 的发展

IPv4 存在的问题：地址空间太小、地址利用率低、地址分配不均、数据报的首部不够灵活。特别是在去除网络地址、广播地址、划分子网的开销、路由器地址、保留地址等地址后，有效的 IP 地址数目比可用的地址总数还要低，难以满足现代网络应用对大量 IP 地址的需要。2011 年 ICANN 正式宣布所有 IPv4 地址分发完毕。同时，IPv4 协议在网络速度、路由表容量、移动性、自动配置、安全性等方面暴露出了诸多局限和不足。为了克服 IP 协议的一些不足，提高语音、视频传输对 QoS 的要求，现在已发展了第 6 版互联网协议 IPv6。

IPv6 有如下改进：IP 地址由 32 位扩充到 128 位，扩大了 IP 地址空间；支持 IP 安全（IPSec）标准，改进端对端的安全；通过减少信息包的丢失，可降低视频会议和 IP 语音（VoIP）系统的不稳定性；采用无类别编址 CIDR，可动态进行地址分配，增强了移动通信能力。随着技术的发展和应用，未来的军事网络将逐步兼容或过渡到 IPv6。

IPv6 具有以下特点：极大的地址空间、分层的地址结构、支持即插即用、灵活的数据报首部格式、支持资源的预分配、认证与私密性、方便移动主机的接入。IPv4 向 IPv6 过渡的方法：使用双协议栈和使用隧道技术。

IPv6 协议较 IPv4 具有绝对的技术优势。

（1）IPv6 具有更大的地址空间。它由 IPv4 的 32 位地址位数增加到 l28 位地址位数。IPv4 提供大约 43 亿个可用地址，而 IPv6 将增长 8×1028 倍。因此，通过 IPv6 技术可以对大到卫星、导弹、飞机、舰船、坦克、火炮等装备系统，小到单兵作战装备甚至是每一颗弹药都分配地址。

（2）IPv6 使用更小的路由表。IPv6 的地址分配一开始就遵循聚类的原则，这使得路由器能在路由表中用一条记录表示一片子网，大大减小了路由器中路由表的长度，提高了路由器转发数据包的速度。

（3）IPv6 增加了增强的组播支持及对流的控制，这使得网络上的多媒体应用有了长足发展的机会，为服务质量保障提供了良好的网络平台。

（4）IPv6 加入了对自动配置的支持。这是对 DHCP 协议的改进和扩展，使得网络（尤其是局域网）的管理更加方便和快捷。

（5）IPv6 具有更高的安全性。IPv6 要求强制实施因特网安全协议 IPSec，并已将其标准化。IPv6 的加密与鉴别选项提供了分组的保密性和完整性，用户可以对网络层的数据进行加密并对 IP 报文进行校验。虽不能杜绝网络攻击，但是比现有的 IPv4 大幅提高了安全性。

（6）更好的头部格式。IPv6 使用新的头部格式，其选项与基本头部分开，如果需要，可将选项插到基本头部与上层数据之间，这就简化和加速了路由选择过程。

（7）允许扩充。如果新的技术或应用需要，IPv6 允许对协议进行扩充。

IPv6 已成为构建安全、可靠、端到端、可升级的网络传输基础设施、实现各种异构网络集成的关键手段。其高度灵活、安全、层次的地址方案，可动态分配地址的特性，对于军事通信网络的建设具有重要意义；其近乎无限的地址空间、灵活的寻址能力，对于实现传感器、移动智能终端、基本作战单元及各个网系、信息系统乃至武器系统平台的入网互联提供了有效支持；其利用 IPSec 安全协议对数据进行加密和对 IP 报文进行校验的措施，能够大大增强 IPv6 军事网络通信的安全性。这些特性使得 IPv6 能更好地满足军事网络系统对网络整体吞

吐量、网络安全性、服务质量、即插即用、移动性和网络组播等的特殊需求。特别是随着互联网、电信网、广电网的“三网合一”，IPv6 将对军事指挥、政工宣传、后装保障等产生重要影响。

4.2 网络互连原理

4.2.1 路由器的作用

相互连接的计算机网络可以组成一个更大的计算机网络，可以使处于不同地理位置的计算机进行通信。但网络互连存在一些共性问题，如不同的寻址方案、不同的最大分组长度、不同的网络接入机制、不同的超时控制、不同的差错恢复方法、不同的状态报告方法、不同的路由选择技术、不同的用户接入控制、不同的服务（面向连接服务和无连接服务）、不同的管理与控制方式等。网络互联必须妥善处理这些问题，才能使不同结构的网络、不同类型的机器之间互相连通，实现更大范围和更广泛意义上的资源共享。

1．路由器要解决的问题

军事广域网以高速光纤网络为基础，以低速程控电话交换网、短波、卫星、数据链等手段为协助，以 IP 传输为主要方式，实现军事信息在各系统、各用户之间的传递。总体上看，接入军事广域网有专线型和交换型两种联网形态，如图 4-6 所示。

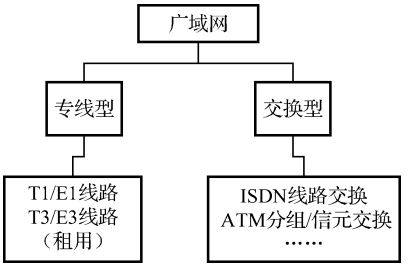


图 4-6　军事广域网的主要连网形态

高速宽带网是现代军事广域网络的重要形式，其节点关系如图 4-7 所示。其中，各级节点实现广域互连的核心设备是路由器。它将某个军事信息系统的内部局域网中的服务器和席位计算机等设备与广域网上的其他信息系统实现互联互通。

可见，路由器是局域网连接到高速宽带广域网络的关键设备，是实现广域网上其他军事系统互连、互通、互操作的基础。之所以需要这样的专门设备，是因为互连的局域网络在体系结构、协议层次及服务等方面或多或少存在着差异。对于异构网络来说，这种差异可能表现在寻址方式、路由选择、最大长度、网络接入机制、用户接入控制、超时控制、差错恢复方法、服务、管理方式等多个方面。

要实现网际互连，就必须消除这些差异。归纳起来，就是要解决如下 3 个问题。

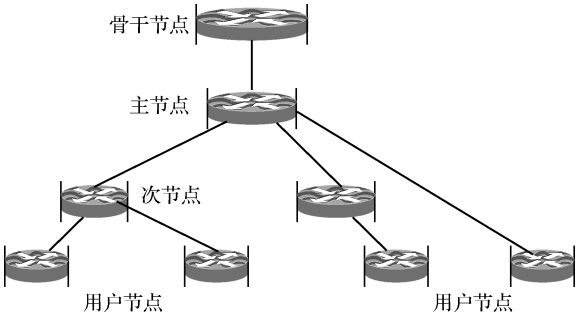


图 4-7 高速宽带通信网的节点关系示意图

（1）路由选择：由于源和目的站不是直接连接的，网络必须将分组从一个节点选择路由传输到另一个节点，最后通过整个网络。

（2）分组交换：路由选择确定了输出端口和下一个节点后，必须使用交换技术将分组从输入端口转发到输出端口，实现输送比特通过网络节点。

（3）拥塞控制：进入网络的通信量必须与网络的传输量相协调，以获得有效、稳定、良好的性能。

路由器就是消除不同网络间的差异、实现多个局域网或网段互连，从而构成广域网络的核心设备。它在广域网络中主要实现分组转发和路由选择功能。所谓“路由”，是指将数据从一个地方传送到另一个地方的行为和动作。路由器就是执行这种行为和动作的机器，是一种连接多个网络或网段的网际设备。它能将不同网络或网段之间的数据信息进行“翻译”，以使它们能够相互“读懂”对方的数据，从而构成一个更大的网络。

2．路由器的主要功能

从 TCP/IP 体系结构看，局域网的体系结构主要涉及物理层和数据链路层两层，而广域网则包含了网络接口层、网络层、运输层和应用层。路由器就工作在网络层，通过选择与控制数据传输的路径，将数据从一个地方传送到另一个地方。其“路由”功能体现在如下方面。

（1）数据转发

在网际间接收节点发来的数据包，然后根据数据包中的目的地址，对照自己缓存中的路由表，把数据包直接转发到目的节点。这是路由器最主要、最基本的路由作用。

（2）为网际间通信选择最合理的路径

如果有几个网络通过各自的路由器连在一起，一个网络中的用户要向另一个网络的用户发出访问请求，路由器就会分析发出请求的源地址和接收请求的目的节点地址中的网络 ID 号，找出一条合适的通信路径。

（3）拆分和合并数据包

因为有时在数据包转发过程中，由于网络带宽等因素，数据包过大，很容易造成网络堵塞。这时，路由器就要把大的数据包根据对方网络带宽状况拆分成若干个小的数据包，到了目的网络的路由器后，目的网络的路由器会将被拆分的数据包合并成一个原来大小的数据包，再根据目的节点的 MAC 地址发给本地网络的节点。

（4）实现不同协议网络之间的连接

目前多数中高档路由器往往都具有支持多通信协议的功能，这样就可以起到了连接两个不

同通信协议网络的作用。如常用 Windows 操作平台所使用的通信协议主要是 TCP/IP 协议，但是如果是 NetWare 系统，则所采用的通信协议主要是 IPX/SPX 协议。一些特殊的协议网段则需要靠支持这些协议的路由器来连接。

（5）防火墙功能（可配置独立 IP 地址的网络管理型路由器）

它能够起到基本的防火墙功能，也就是它能够屏蔽内部网络的 IP 地址，自由设定 IP 地址、通信端口过滤，使网络更加安全。

4.2.2　路由选择算法

1．路由选择问题

当分组从一个主机传输到另一个主机时，可以通过很多条路径传输。路由器的主要工作就是为经过路由器的每个数据帧寻找一条最佳传输路径，并将该数据有效地传送到目的站点。

路由算法代表了选择最佳路径的策略，是路由器的关键所在。为了完成这项工作，路由器中有一张路由表（Routing Table），供路由选择时使用。路由表中保存着子网的标志信息、网上路由器的个数和下一个路由器的名字等各种传输路径的相关数据。

为了实现路由选择，路由算法必须随时了解网络状态信息。

（1）路由器必须确定它是否激活了对该协议组的支持。

（2）路由器必须知道目的地网络。

（3）路由器必须知道哪个外出接口是到达目的地的最佳路径。

2．路由算法功能

到达目的地的最佳路径的选择依据是路由算法计算得到的度量值。路由算法是网络层软件的一部分，它负责确定路由器收到的分组应该被传送到哪一条输出线路上。路由算法在路由协议中起着至关重要的作用，采用何种算法往往决定了最终的寻径结果。

一个好的路由算法通常具备以下能力。

（1）能迅速而准确地传递分组：如果目的主机存在，它必须能够找到通往目的地的路由，而且路由搜索时间不太长。

（2）能适应由节点或链路故障而引起的网络拓扑结构的变化：在实际网络中，设备和传输链路都可能随时出现故障。因此路由算法必须能够适应这种情况，在设备和链路出现故障时，可以自动地重新选择路由。

（3）能适应源和目的主机之间业务负荷的变化：业务负荷在网络中是动态变化的。路由算法应该能够根据当前业务负载情况来动态地调整路由。

（4）能使分组避开暂时拥塞的链路：路由算法应该使分组尽量避开拥塞严重的链路，最好还能平衡每段链路的负荷。

（5）能确定网络的连通性：为了寻找最优路由，路由算法必须知道网络的连通性和各个节点的可达性。

（6）低开销：通常路由算法需要各个节点交换控制信息来得到整个网络的连通性等信息。在路由算法中应该使这些控制信息的开销尽量小。

3．路由算法分类

路由算法分为非自适应算法和自适应算法两大类。非自适应算法不会根据当前测量或估计的流量和拓扑结构来调整它们的路由决策，这个过程也称为静态路由。相反，自适应算法则会改变它们的路由决策，以反映出拓扑结构的变化，通常也会反映出流量的变化情况，这个过程称为动态路由。在所有的分组交换网络中都使用了某些自适应性路由选择技术，路由选择的决定将随着网络情况的变化而变化。在自适应路由选择技术中，影响路由选择的主要因素有以下两个方面：一是当一个节点或节点间链路出故障时，它就不能再被用作路径的一部分；二是当网络的某一部分出现严重拥塞时，应使分组选择绕开拥塞区路径而不是通过拥塞区路径。

（1）静态路由算法

在路由器中设置固定的路由表。首先根据网络的拓扑结构确定路径，然后将这些路径填入路由表中，除非网络管理员干预，否则静态路由不会发生变化。静态路由的优点是简单、高效、可靠。由于静态路由不能对网络的改变做出反映，这种路由算法适合网络拓扑结构比较稳定而且网络规模比较小的网络。当网络比较大时，静态路由算法就不太适用了，因为它不能根据网络的故障和负载的变化来做出快速反应。

（2）动态路由算法

网络中的路由器之间相互传递路由信息，利用收到的路由信息更新路由表。路由器通过与其邻居通信来不断学习网络的状态。因此网络的拓扑结构变化可以最终传播到整个网络中的所有路由器。根据这些收集到的信息，每个路由器都可以计算出到达目的主机的最佳路径。动态路由能实时地适应网络结构的变化。如果路由更新信息表明发生了网络变化，路由选择软件就会重新计算路由，并发出新的路由更新信息。这些信息通过各个网络引起各路由器重新启动其路由算法，并更新各自的路由表以动态地反映网络拓扑变化。所以，动态路由适用于网络规模大、网络拓扑复杂的网络，但由于各种动态路由算法会不同程度地占用网络带宽和 CPU 资源，因而会增加路由器的复杂性，增大路由选择时延。

复杂的路由算法可能采用多种度量来选择路由，通过一定的加权运算，将它们合并为单个的复合度量，再填入路由表中，作为寻找最佳路径的依据。常使用的度量有：路径长度、可靠性、时延、带宽、负载、通信成本等。复杂路由算法主要分链路状态算法和距离向量算法两类。

（1）链路状态算法也称最短路径算法。发送路由信息到网上所有的节点，然而对于每个路由器，仅发送它的路由表中描述了其自身链路状态的那一部分。它发送给网络中其他路由器的更新信息较少，算法收敛较快，不易产生路由循环，但需要更强的 CPU 和更多的内存空间。

（2）距离向量算法也称为 Bellman-Ford 算法。要求每个路由器发送其路由表的全部或部分信息，但仅发送到邻近节点上。它会发送大量更新信息至邻接路由器。由于发送的更新信息较多，易于产生路由循环，但所需的 CPU 能力和内存空间比链路状态算法低些。

路由算法根据控制方式还可以分为集中路由算法和分布式路由算法。

（1）集中路由算法。在集中式路由算法中，所有可选择的路由都由一个网控中心算出，并且由网控中心将这些信息加载到各个路由器中。这种算法只适用于小规模的网络。

（2）分布式路由算法。在分布式路由算法中，每个路由器都进行各自的路由计算，并且通过路由消息的交换来互相配合。这种算法可适应大规模的网络，但是容易产生一些不一致的路由结果。而这些不同路由器计算的不同路由结果可能会导致路由环路的产生。

静态路由和动态路由有各自的特点和适用范围，动态路由常作为静态路由的补充。在一个

路由器中，可同时配置静态路由和一种或多种动态路由。它们各自维护的路由表都提供给转发程序，但这些路由表的表项间可能会发生冲突，这种冲突可通过配置各路由表的优先级来解决。通常静态路由具有默认的最高优先级，当一个分组在路由器中进行寻径时，路由器首先查找静态路由，如果查到则根据相应的静态路由转发分组，否则再查找动态路由进行转发。如果其他路由表的表项与静态路由相矛盾，则均按静态路由转发。

4.2.3　典型路由协议

1．信息路由原则

路由协议是路由选择协议的简称。路由器之所以能在不同网络之间起到“翻译”的作用，是因为它不再是一个纯硬件设备，而是具有相当丰富路由协议的软、硬结合的设备。路由器通过路由协议实现不同网段或网络之间的相互“理解”，实现分组在不同网段或网络之间的路由转发。

为提高网络的可控可管和抗毁顽存能力，信息路由应遵循以下原则。

（1）为提高网络路由的管控能力，防止由于路由不一致对时延、时延抖动、乱序等性能指标的影响，网络应遵循路由一致的选路原则。在网络异常情况下（如网络严重受损等），则保证自治系统内部的路由一致。

（2）主干、地区和重要的接入节点具有迂回和备份路由，信息路由按主用、迂回和备份路由的顺序依次选择。迂回路由用于防止链路失效，备份路由用于防止上连节点失效。节点下辖的同级节点之间构成迂回路由，节点连接到非所属的上级节点或非同层面的节点构成备份路由。

通过划分区域的方式执行上述信息路由原则。也就是将功能或地理位置相同的路由器划分在一个区域内，以降低运行路由协议对路由器性能的要求，也便于隔离拓扑变化，并且可以减少路由震荡对整个自治系统的影响。

计算机网络中，具有统一管理机构、统一路由策略的网络称为自治系统（Autonomous System，AS）。根据是否在一个自治域内部使用，动态路由协议分为内部网关协议（IGP）和外部网关协议（EGP）。自治域内部采用的路由选择协议称为内部网关协议，常用的有路由信息协议（Routing Information Protocol，RIP）、开放最短路径优先协议（Open Shortest Path First，OSPF）。外部网关协议主要用于多个自治域之间的路由选择，常用的是边界网关协议（Border Gateway Protocol，BGP）和 BGP-4。RIP、OSPF 和 BGP 路由选择协议的主要特点如表 4-3 所示。

表 4-3　典型路由协议的主要特点

主 要 特 点	RIP	OSPF	BGP
网关协议	内部	外部	外部
路由表内容	目的网，下一站，距离	目的网，下一站，距离	目的网，完美路由
最优通路依据	跳数	费用	多种策略
算法	距离矢量	链路状态	距离矢量
传送方式	运输层 UDP	IP 数据报	建立 TCP 连接
其他	简单；效率低；跳数为 16，不可达；好消息传得快，坏消息传得慢	效率高；路由器频繁交换信息，难维持一致性；规模大，统一度量，可达性	

2．RIP

路由信息协议（RIP）是一种应用较早、使用广泛的自治系统内部网关协议。它是典型的距离向量算法协议，简单、可靠，便于配置，适用于小型网络。RIP 路由以距离最短 HOPS 的路径为路由。路由器收集所有可到达目的地的不同距离，并且保存到达每个目的地的最小距离的路径信息，除到达目的地的最佳路径外，任何其他信息均予以丢弃。同时路由器也把所收集的路由信息用 RIP 协议通知相邻的其他路由器，供其邻接路由器更新有关路由信息，使正确的路由信息逐渐扩散到全网。

这里，“距离”是指分组经过网络的个数，也指“跳过（hop）”路由器的个数。RIP-1 版本的最大距离数是 15，RIP-2 版本的最大距离数是 128，大于 15/128 则认为不可到达。因此，在大的网络系统中，跳数很可能超过规定值，使用 RIP 是很不现实的。RIP 有三个时钟，分别是路由更新时钟（每 30 秒）、路由无效时钟（每 90 秒）、路由取消时钟（每 270 秒）。RIP 每隔 30 秒才进行信息更新，路由信息广播容易造成网络广播风暴，因此，在大型网络中，坏的链路信息可能要花很长时间才能传播过来，路由信息的稳定时间可能更长，并且在这段时间内可能产生路由环路。

3．OSPF

20 世纪 80 年代中期，RIP 已不能适应大规模异构网络的互连，一种基于链路状态的路由协议 OSPF（Open Shortest Path First）随之产生。它是网间工程任务组织（Internet Engineering Task Force，IETF）于 1987 年开发的一种链路状态路由协议。OSPF 能够适应大型全局 IP 网络的扩展，成为单一自治系统内部主要的路由协议。

为了适应大型网络，与 RIP 不同，OSPF 将一个自治域再划分为多个区域，按照一定的 0SPF 路由法则组合在一起的一组网络或路由器的集合称为区域。每个区域都有一个区域号，当网络中存在多个区域时，必须存在 0 区域，它是骨干区域，所有其他区域都通过直接或虚链路连接到骨干区域上。为了优化操作，各区域所包含的路由器不应超过 70 个。一个物理上的地区网络原则上组成一个 OSPF 普通区域。

OSPF 需要每个路由器向其同一管理域的所有其他路由器发送链路状态广播信息。在 OSPF 的链路状态广播中包括所有接口信息、所有量度和其他一些变量。利用 OSPF 的路由器首先必须收集有关的链路状态信息，并根据一定的算法计算出到每个节点的最短路径。而基于距离向量的路由协议（RIP）仅向其邻接路由器发送有关路由更新信息。

OSPF 协议的特性包括：支持 VLSM（可变长子网掩码）、快速收敛、低网络利用、高级路由选择及可用组播传送报文等。每个 OSPF 路由器只维护所在区域的完整的链路状态信息，由于没有路由跳数的限制，使用组播更新变化的路由和网络信息，OSPF 路由收敛速度较快。通过策略路由、更改度量值及采用 OSPF 负载均衡等方法，实现网络最优路径选择。

分区域的 OSPF 有两种类型的路由选择方式：当源和目的地在同一区域时，采用区域内路由选择；当源和目的地在不同区域时，采用区间路由选择。这就大大减少了网络开销，并增强了网络的稳定性。当一个区域内的路由器出故障时并不影响自治域内其他区域路由器的正常工作，这也给网络的管理、维护带来了方便。

4．BGP

BGP 用于允许不同的自治系统中的路由器能够交换路由选择信息，这些路由器在标准中被称为网关。BGP 是 TCP/IP 互联网的外部网关协议，用来在自治系统之间传递路由信息，从设计上避免环路的发生，具有丰富的路由策略，目前广泛使用的最新版本是 BGP-4，它既不是基于纯粹的链路状态算法，也不是基于纯粹的距离向量算法，它的主要功能是与其他自治域的 BGP 交换网络可达信息。各个自治域可以运行不同的内部网关协议。BGP 更新信息包括网络号/自治域路径的成对信息。自治域路径包括到达某个特定网络须经过的自治域串，这些更新信息通过 TCP 传送出去，以保证传输的可靠性。

在互联网中，交换路由选择信息的路由器称为邻站，同属一个自治系统的邻站称为内部邻站，分属不同自治系统的邻站称为外部邻站。BGP 用于外部邻站交换路径信息。一般情况下，BGP 邻站位于同一个网络上，这个网络本身属于两个自治系统。BGP 协议具有三大功能：第一，邻站获取，路由器可以请求另一自治系统中的某路由器作为自己的外部邻站（BGP 邻站），以便互换路由选择信息；第二，邻站可达，一旦建立了邻站的关系，互相就必须不断发送报文，测试和维持邻站关系。第三，网络可达，BGP 邻站之间必须及时交换各自的路由选择信息，包含它可以到达的网络和最佳路由信息。

BGP 可以分为两种不同的模式：外部 BGP（External BGP，EBGP）和内部 BGP（Internal BGP，IBGP）。外部 BGP 在自治系统之间交换网络层可达信息（Network Layer Reachability Information，NLRI），而内部 BGP 在自治系统内部交换可达信息。为了满足 Internet 日益扩大的需要，BGP 还在不断发展。在最新的 BGP-4 中，还可以将相似路由合并为一条路由。

4.2.4　路由器工作原理

路由器通过路由协议算法识别另一个网络，首先要识别的就是对方网络的路由器 IP 地址的网络 ID，看是不是与目的节点地址中的网络 ID 号相一致。如果是，就向这个网络的路由器发送，接收网络的路由器在接收到源网络发来的报文后，根据报文中所包括的目的节点 IP 地址中的主机 ID 号来识别是发给哪一个节点的，然后再直接发送。

当 IP 子网中的一台主机发送 IP 分组给同一 IP 子网的另一台主机时，它将直接把 IP 分组送到网络上，对方就能收到。而要送给不同 IP 于网上的主机时，它要选择一个能到达目的子网的路由器，把 IP 分组送给该路由器，由路由器负责把 IP 分组送到目的地。如果没有找到这样的路由器，主机就把 IP 分组送给一个称为“默认网关（default gateway）”的路由器上。“默认网关”是每台主机的一个配置参数，它是接在同一个网络上的某个路由器端口的 IP 地址。

路由器转发 IP 分组时，只根据 IP 分组目的 IP 地址的网络号部分选择合适的端口，把 IP 分组送出去。同主机一样，路由器也要判定端口所接的是否是目的子网，如果是，就直接把分组通过端口送到网络上；否则，也要选择下一个路由器来传送分组。路由器也有它的默认网关，用来传送不知道往哪儿送的 IP 分组。这样，通过路由器把知道如何传送的 IP 分组正确转发出去，不知道如何传送的 IP 分组送给“默认网关”路由器，这样一级级地传送，IP 分组最终将送到目的地，送不到目的地的 IP 分组则被网络丢弃。

路由动作包括两项基本内容：寻径和转发。寻径即判定到达目的地的最佳路径，由路由选择算法来实现。为了判定最佳路径，路由选择算法必须启动并维护包含路由信息的路由表，其

中路由信息依赖于所用的路由选择算法而不尽相同。路由选择算法将收集到的不同信息填入路由表中，根据路由表可将目的网络与下一站的关系告诉路由器。路由器间互通信息，进行路由更新，更新维护路由表使之正确反映网络的拓扑变化，并由路由器根据量度来决定最佳路径。这就是路由选择协议，如 RIP、OSPF、BGP 等。

转发即沿路由算法得到的最佳路径传送信息分组。路由器首先在路由表中查找，判明是否知道如何将分组发送到下一个站点（路由器或主机），如果路由器不知道如何发送分组，通常将该分组丢弃；否则就根据路由表的相应表项将分组发送到下一个站点，如果目的网络直接与路由器相连，路由器就把分组直接送到相应的端口上。

为了更清楚地说明路由器的工作原理，现在假设有一个如图 4-8 所示的简单网络。

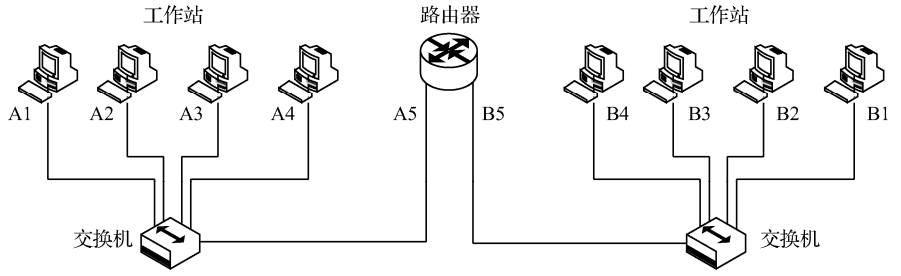


图 4-8　用路由器连接两个网段示意图

其中一个网段网络 ID 号为“A”，在同一网段中有 4 台终端设备连接在一起，这个网段的每个设备的 IP 地址分别假设为 A1、A2、A3 和 A4。连接在这个网段上的一台路由器是用来连接其他网段的，路由器连接于 A 网段的端口 IP 地址为 A5。同样路由器连接另一网段为 B 网段，这个网段的网络 ID 号为“B”，连接在 B 网段的另外几台工作站设备的 IP 地址设为 B1、B2、B3、B4，同样连接于 B 网段的路由器端口的 IP 地址设为 B5。

在这样一个简单的网络中同时存在着两个不同的网段，如果 A 网段中的 A1 用户想发送一个数据给 B 网段的 B2 用户，有了路由器就非常简单了。

首先，A1 用户把所发送的数据及发送报文准备好，以数据帧的形式通过左边的交换机广播发给同一网段的所有节点（交换机因为不能识别这个地址采取广播方式），路由器在侦听到 A1 发送的数据帧后，从中分析出目的节点的 IP 地址信息（路由器在得到数据包后总是要先进行分析），得知不是本网段的地址，就把数据帧接收下来，根据其路由表进一步分析可知，接收节点的网络 ID 号与 B5 端口的网络 ID 号相同。这时，路由器的 A5 端口就直接把数据帧发给路由器的 B5 端口。B5 端口再根据数据帧中的目的节点 IP 地址信息中的主机 ID 号来确定最终目的节点为 B2，然后发送数据到右边的交换机，该交换机再将数据帧发送给 B2 节点，从而将节点 A1 发送的数据发送给节点 B2，由此顺利地到达目的节点，这样一个完整的数据帧的路由转发过程就完成了。

4.2.5　路由交换机的特点

路由交换机就是常说的三层交换机。它把支持 VLAN 的传统交换机和路由器的功能集成在一个设备中，既有二层交换功能又有三层路由功能。

1．路由交换机提出的原因

简单地说，路由交换机就是具有路由功能的交换机，提出的原因主要有以下几点：

（1）二层交换技术极大地提升了以太网的性能，但仍然不能完全满足局域网的需要；

（2）交换式以太网采取划分逻辑子网（VLAN）的方式，才能将广播和本地流量限制在一定的范围内；

（3）VLAN 间的互通传统上需要路由器来完成，而路由器的转发速度容易成为网络瓶颈；

（4）局域网内的业务流遵循“80/20 规则”：用户数据流量的 80% 在本地网段，只有 20% 的数据流量通过路由器进入其他网段。而随着网络间业务流的增加，许多业务遵循“20/80 规则”，80%的流量需要跨越 VLAN，使得路由器不堪重负。

2．路由交换机的功能模型

三层交换机的功能原理如图 4-9 所示。图中右边是一个三层交换机，其实现的功能等同于左边一个 VLAN 二层交换机和路由器组成的网络。

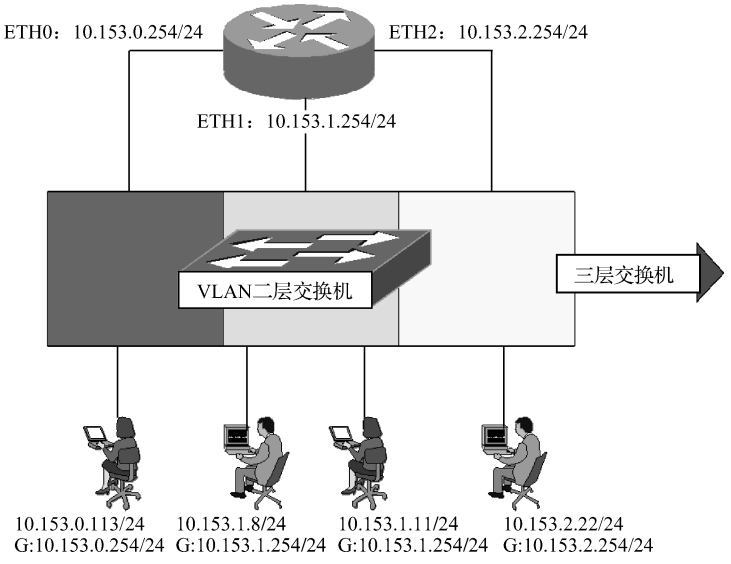


图 4-9　三层交换机功能模型

三层交换机的功能分别通过二层 VLAN 转发引擎和三层转发引擎两部分来实现：二层 VLAN 引擎与支持 VLAN 的二层交换机的二层转发引擎是相同的，是用硬件支持多个 VLAN 的二层转发；三层转发引擎使用硬件 ASIC 技术实现高速 IP 转发，因此比传统路由器转发效率高、时延低、成本低。

三层交换机对应到 IP 网络模型中，每个 VLAN 对应一个 IP 网段，三层交换机中的三层转发引擎在各个网段（VLAN）间转发报文，实现 VLAN 之间的互通，因此三层交换机需要对路由表进行更新和维护，这种路由功能通常叫作 VLAN 间路由（Inter-VLAN Routing）。

对应于二层交换引擎，三层交换机的交换引擎如图 4-10 所示。

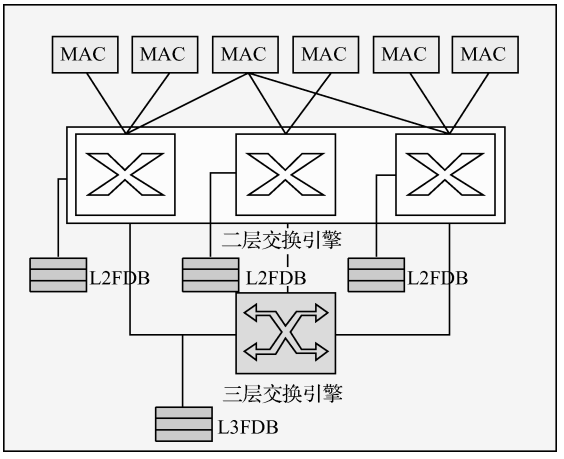


图 4-10　三层交换引擎

在二层上，VLAN 之间是隔离的，VLAN 内主机可以互通，这一点跟二层交换机中的交换引擎的功能相同。一般来说，三层交换机的每个 VLAN 对应一个网段，不同的 IP 网段之间的访问要跨越 VLAN，要使用三层交换引擎提供的 VLAN 间路由功能。在使用二层交换机和路由器的组网中，每个需要与其他 IP 网段（VLAN）通信的 IP 网段（VLAN）都需要使用一个路由器接口做网关。给 VLAN 指定路由接口的操作，实际上就是为 VLAN 指定一个 IP 地址、子网掩码和 MAC 地址，MAC 地址是在设备制造过程中分配的，在配置过程中由交换机自动配置。二者最大的区别在于三层交换采用 ASIC 硬件进行包转发，而传统路由器采用 CPU 进行包转发。

3．路由交换机的转发流程

究竟什么时候选择二层交换、什么时候选择三层路由，这涉及 IP 网络通信的基本规则。每个网络主机、工作站或服务器都有自己的 IP 地址和子网掩码。当主机与服务器进行通信时，根据自身的 IP 地址和子网掩码及服务器的 IP 地址来确定服务器是否和自己处于相同的网段：

（1）如果判定在相同网段内，则直接通过地址解析协议（ARP）查找对方的 MAC 地址，然后把对方的 MAC 地址填入以太网帧头的目的 MAC 地址域，将报文发送出去，通过二层交换实现通信；

（2）如果判定在不同的网段内，主机就会自动借助网关来进行通信。主机首先通过 ARP 来查找设定的网关的 MAC 地址，然后把网关的 MAC 地址（而不是对方主机的 MAC 地址，因为主机认为通信中的端主机不是本地主机）填入以太网帧首部的目的 MAC 地址域，将报文发送给网关，通过三层路由实现通信。

对于三层交换机，接收到一个报文后选择二层转发还是三层转发，判断的依据主要是：报文的目的 MAC 地址。如果该目的 MAC 地址和设备内某个 VLAN 指定的路由接口 MAC 地址相同，则进行三层转发，否则在 VLAN 内部进行二层转发。当然，严格地说，设备对报文的目的 IP 也需要进行判断，因为报文有可能是直接发送给该 VLAN 接口的。

下面具体介绍三层交换机的转发流程，以图 4-11 为例。

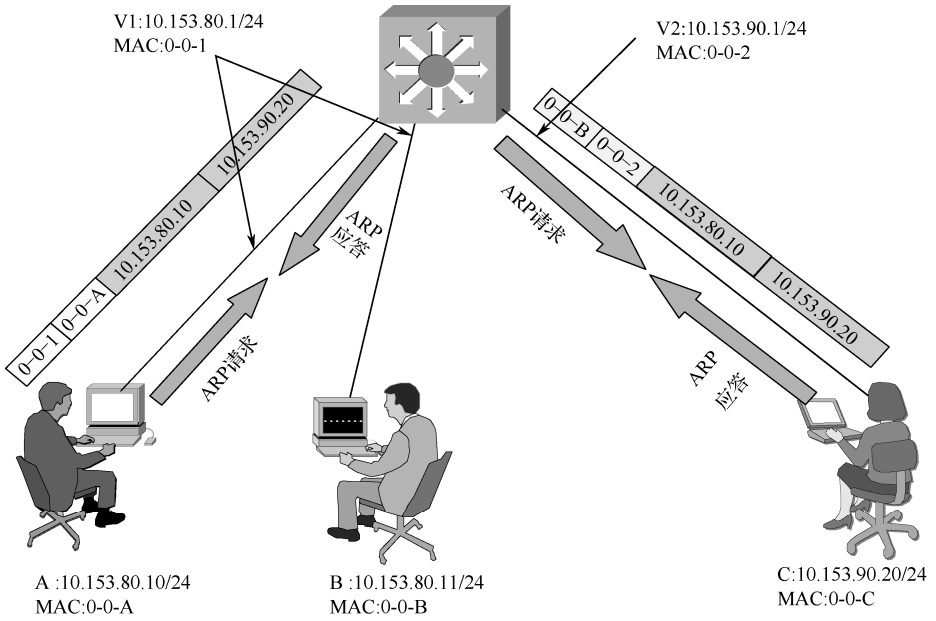


图 4-11　三层转发流程

交换机上划分了两个 VLAN，在 VLAN 1、VLAN 2 上配置了路由接口用来实现 VLAN 1 和 VLAN 2 之间的互通。A、B 的网关是 VLAN 1 虚接口地址，C 的网关是 VLAN 2 虚接口地址。

（1）二层交换过程

以 A 向 B 发起 ping 请求为例。A 检查报文的目的 IP 地址，发现和自己在同一个网段：

① A---->B　ARP 请求报文，该报文在 VLAN1 内广播；

② B---->A　ARP 回应报文；

③ A---->B　ICMP 请求；

④ B---->A　ICMP 应答。

（2）三层转发过程

以 A 向 C 发起 ping 请求为例。A 检查要通信 C 的目的 IP 地址，发现和自己不在同一个网段，因此要借助 A 的网关来和 C 通信：

① A 向交换机的 VLAN1 虚接口发送 ARP 请求报文，在 VLAN1 内广播请求 A 的 MAC 地址；

② 网关向 A 回应 ARP 应答报文；

③ A 向交换机发送 ICMP 请求（目的 MAC 是 VLAN1 虚接口的 MAC，源 MAC 是 A 的 MAC，目的 IP 是 C 的 IP，源 IP 是 A 的 IP）；

④ 交换机收到报文后根据目的 MAC 判断出是三层报文。检查报文的目的 IP 地址，发现在自己的直连网段（VLAN2 虚接口所在网段）；

⑤ 交换机在 VLAN2 内广播 C 的 ARP 请求报文，请求 C 的目的 MAC；

⑥ C 向交换机发送 ARP 回应报文；

⑦ 交换机通过 VLAN 2 虚接口向 C 转发 ICMP 请求（目的 MAC 是 C 的 MAC，源 MAC 是 VLAN2 虚接口的 MAC，目的 IP 是 C 的 IP，源 IP 是 A 的 IP）报文。同步骤④相比，报文

的 MAC 头进行了重新封装，而 IP 层以上的字段基本不变；

⑧ C 向 A 回应 ICMP 应答，以后的处理同 ICMP 请求的过程基本相同。

需要说明的是，以上各步处理中，如果 ARP 表中已经有了相应的表项，则不会给对方发 ARP 请求报文。

4．路由器与三层交换机的差异

前面对三层转发过程进行了简单阐述。实际上，三层交换机在接收到一个报文后，在需要进行三层转发时，其选路和转发过程还是比较复杂的。为了便于理解和对比，先了解一下路由器的最长匹配选路过程。以图 4-12 为例，打钩的第 2 项是最长匹配项。

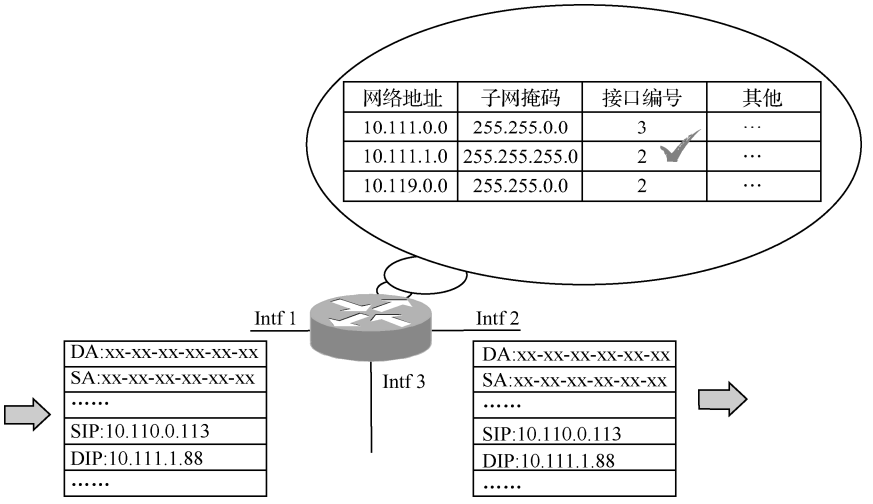


图 4-12　路由器的最长匹配转发

（1）路由器的路由步骤

① 根据报文的目的地址，与路由项进行匹配操作。

匹配的动作是用报文目的地址与路由项的子网掩码进行“与”。在图 4-12 中，目的 IP 地址 10.111.1.88 和各表项子网掩码“与”的结果如下：

10.111.1.88 & 255.255.0.0 = 10.111.0.0

10.111.1.88 & 255.255.255.0 = 10.111.1.0

10.111.1.88 & 255.255.0.0 = 10.111.0.0

② 如果“与”的结果和路由项中网络地址相同，则认为路由匹配。所有匹配项中子网掩码位数最长的为最佳匹配项，报文从该表项对应接口发送出去，如图 4-19 所示。

③ 如果找不到匹配项，则根据默认路由 0.0.0.0/0 进行转发。

④ 如果没有默认路由则报文被丢弃。

上述路由选择过程称之为最长匹配。路由表是根据静态路由协议和动态路由协议生成的，选择最优路由表项后生成的是转发表。路由器实际是利用转发表转发报文的。

（2）三层交换机的路由步骤

那么交换机的选路和路由器有什么异同？总的来说，交换机和路由器一样，也是由软件来维护路由表和转发表，但交换机的报文选路转发通过 ASIC 硬件进行，效率大大超过路由器。而且交换机除了支持与路由器相同的最长匹配转发外，还支持精确匹配转发。

精确匹配转发主要依靠 L3FDB，其作用类似于二层交换机“Cache”的 MAC 地址表，如图 4-13 所示，打钩的第 1 项是精确匹配项。其步骤是：

① 交换机根据报文的目的 IP 在 L3FDB 表中进行查找；

② 对于能够在此“Cache”命中的报文，直接根据表项的端口信息进行转发；

③ 不能在“Cache”命中的报文将被送到 CPU 进行软件路由，路由的原理和路由器完全相同的最长地址匹配；

④ 软件路由后将把该目的 IP 添加到 L3FDB 表中；

⑤ 如果表项长期不被刷新则被老化掉。

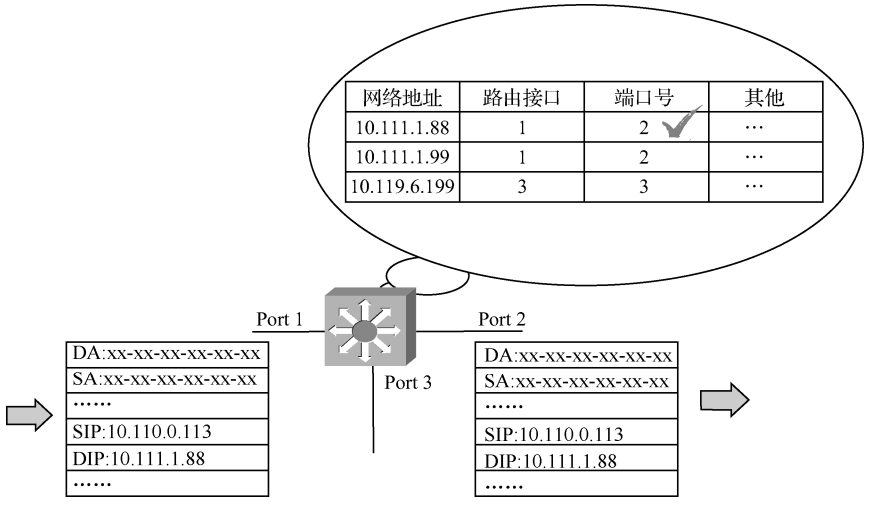


图 4-13　三层交换机转发——精确匹配

因此，通过多次地址学习就可以把表项逐一加进来，这样后续的流量就可以直接 Cache 命中，不需要软件路由。这就是三层交换机所谓的“一次路由，多次交换”。但从实际应用看，精确匹配转发有一定局限。因为它对于每一个目的 IP 在 L3FDB 表中都会存在一个表项，对硬件资源要求很高。所以，现有三层交换机也都支持最长匹配转发。

三层交换机的最长匹配转发原理如图 4-14 所示，打钩的第 2 项是其最长匹配项。其步骤是：

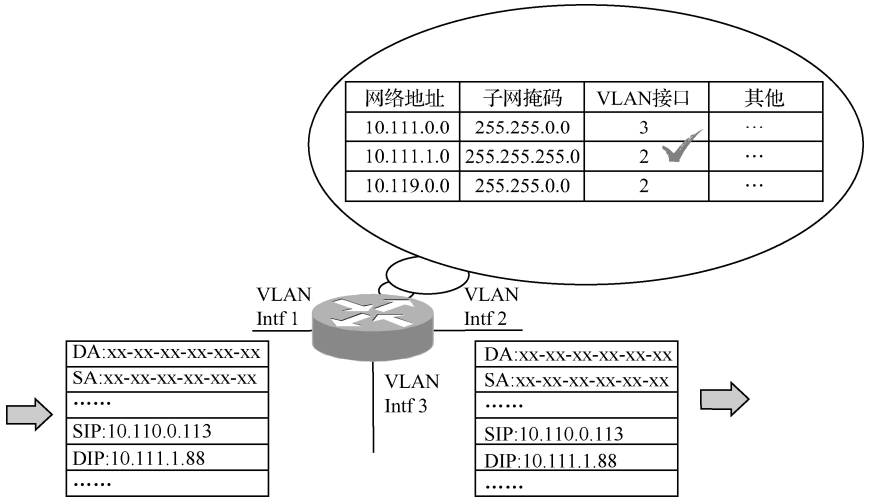


图 4-14　三层交换机转发——最长匹配

① 最长匹配转发也依赖于 L3FDB；

② L3FDB 转发项通过 FIB 表项下发建立起来；

③ 对于能够在此“Cache”命中的报文，则直接进行转发；

④ 不能在“Cache”命中的报文将被转发到 CPU 进行软件路由，路由的原理和路由器完全相同的最长地址匹配。

（3）路由接口和物理端口的差异

无论对路由器还是对三层交换机而言，接口都存在路由接口和物理接口的概念。路由接口是挂接在 IP 协议栈下的逻辑接口，每个接口都对应一个 IP 网段，通常称为 Interface。物理接口在机箱外面，看得见、摸得着，是能插电缆的实际接口，通常称为 Port。

表 4-4 给出了路由器和三层交换机的特点对比。

表 4-4 路由器和三层交换机的特点对比

项　目	路 由 器	三层交换机
端口类型	非常丰富，几乎支持所有通信端口	主要支持以太网，骨干设备上支持 POS 和 ATM
转发实现途径	主要由 CPU 软件实现	由硬件 ASIC 实现转发
路由算法	最长匹配	精确匹配或最长匹配
包转发率	低	高
成本	高	低
二层交换	不支持	支持
接口对应关系	三层接口和物理接口一一对应	一个 VLAN 三层接口可以包含多个物理接口

从路由器角度理解的端口和从三层交换机角度理解的端口有所不同。路由器一般不提供端口之间的二层转发功能，因此路由接口和物理接口实际上是一一对应的关系，常不做区别。在配置的时候，好像 IP 地址都是直接配置在物理端口上的。

而三层交换机在不同的物理端口之间还提供二层交换功能。VLAN 内部通过二层交换通信，VLAN 之间通过三层路由来通信。路由接口与 VLAN 有对应关系，每个 VLAN 可能对应多个物理端口，因此路由接口和物理端口没有一一对应的关系。

4.3 广域网络技术

广域网可以分为公共传输网络和专用传输网络，也包括无线广域网络。20 世纪 80 年代，远程数据通信主要发展了基于模拟电话线路的公用分组交换网 X.25，20 世纪 90 年代初发展了采用光纤作为传输介质的帧中继（Frame Relay，FR）网络，这两种都是网络接入速度小于 64Kbps 的窄带数据通信网。为提供语音、数据、图像等各种业务传输能力，20 世纪 80 年代进一步发展了综合业务数字网（Integrated Services Digital Network，ISDN），以便能够一同传递语音、数据、多媒体等各种业务，同时为了满足对各种宽带和可变速率业务的需要，后续又提出了宽带综合业务数字网（B-ISDN）。实现快速分组交换的（Asynchronous Transfer Mode，ATM）技术，就是国际电联（ITU-T）于 1988 年正式命名并推荐为 B-ISDN 的数据传递模式。X.25 网、帧中继网和 ATM 网等实际上都为了解决 IP 层下面的数据链路建立与传输问题。

新一代宽带 IP 网络技术有 IP over ATM、IP over SDH、IP over WDM 等。IP over ATM 融合了 IP 和 ATM 技术的特点，发挥 ATM 支持多业务、提供 QoS（服务质量保证）的技术优势。IP over SDH 直接在 SDH 上传送 IP 业务，对 IP 业务提供了完善的支持，提高了效率。IP over WDM 采用高速路由交换机设备和 DWDM（密集波分复用）技术，极大地提高了网络带宽，对不同码率、数据帧格式的业务提供全面支持。以 IP 分组为核心的数据通信已经成为军队信息化平台建设的技术出发点，全面有效地支持 IP 业务是军事系统的发展方向。

宽带骨干网络主要通过光缆和双绞线连接，对部分无法通过宽带入网的系统，使用专线、卫星通信、短波等方式入网。

4.3.1　宽带 IP 网络

高速宽带 IP 网络是指交换设备、中继线路、接入设备和用户终端都是宽带的，集数据、语音、视频服务为一体。它以 IP 和 SDH、ATM 等技术为基础，集成与发展了宽带 IP 网络传输技术、宽带 IP 网络接入技术。IP over ATM 充分利用已经存在的 ATM 网络和技术，适合于提供高性能的综合通信服务，避免不必要的重复投资，是传统电信服务商的较好选择。IP over SDH 去掉了 ATM 设备，投资少、见效快而且线路利用率高，是发展高性能 IP 业务的较好选择。在外围网络以千兆位以太网成为主流的情况下，IP over DWDM 将是宽带 IP 主干网的主流。

1．IP over ATM（POA）

IP over ATM（POA）是 IP 技术与 ATM 技术的结合，它是在 IP 路由器之间（或路由器与交换机之间）采用 ATM 网进行传输。

IP over ATM 的基本原理和工作方式为：将 IP 数据包在 ATM 层全部封装为 ATM 信元，以 ATM 信元的形式在信道中传输。当网络中的交换机接收到一个 IP 数据包时，它首先根据 IP 数据包的 IP 地址通过某种机制进行路由地址处理，以便按路由转发。随后，按已计算的路由在 ATM 网上建立虚电路（VC）。以后的 IP 数据包将在此虚电路 VC 上以直通（Cut-Through）方式传输而不再经过路由器，从而有效地解决了 IP 的路由器瓶颈问题，并将 IP 包的转发速度提高到交换速度。

IP over ATM 的优点：

（1）技术本身能提供 QoS 保证，具有流量控制、带宽管理、拥塞控制功能及故障恢复能力，这些是 IP 所缺乏的，因而 IP 与 ATM 技术的融合，也使 IP 具有了上述功能，这样既提高了 IP 业务的服务质量，又能够保障网络的高可靠性；

（2）适用于多业务，具有良好的网络可扩展能力，并能对 IPX 等其他网络协议提供支持。

IP over ATM 的缺点：

（1）网络体系结构复杂，分割 IP 数据包后会加入大量的头信息，从而需要传输更多的数据，造成很大的带宽浪费；

（2）由于传统的 IP 只工作在 IP 子网内，ATM 路由协议并不知道 IP 的 QoS、多播等业务需求，ATM 不能够保证高效率地传送 IP 业务，在 ATM 网络中存在着扩展性和优化路由的问题。

2．IP over SDH（POS）

IP over SDH 也称 Packet over SDH（POS），是 IP 技术与 SDH 技术的结合，是在 IP 路由器

之间(或路由器与交换机之间)以 SDH 网络作为 IP 数据网络的物理传输网络。实现 IP over SDH 技术需要高速路由器和 PPP 协议,利用 PPP 链路封装协议对 IP 数据包进行封装,然后按照 SDH 标准的帧结构封装成 SDH 帧在光纤中传输，疏导干线上的高速率数据流。

IP over SDH 的优点：

（1）IP 与 SDH 技术的结合是将 IP 数据报通过点到点协议直接映射到 SDH 帧，其中省掉了中间的 ATM 层，从而简化了 IP 网络体系结构，提供更高的带宽利用率，提高了数据传输效率，降低了成本。

（2）保留了 IP 网络的无连接特征，易于兼容各种不同的技术体系和实现网络互连，更适合组建专门承载 IP 业务的数据网络。

（3）能利用 SDH 技术本身的环路，故可利用自愈合（Self-healing Ring）能力达到链路纠错；同时利用 OSPF 协议防止设备和线路故障造成的网络停顿，提高网络的稳定性和可靠性。

IP over SDH 的缺点：

（1）IP over SDH 中的 PPP 本身无寻址和路由能力，网间必须配置点到点链路及冗余链路，所以 SDH 链路带宽是独占而共享的，而 ATM 网络具有完整的寻址和路由连接功能；

（2）SDH 具有光纤被切断时的保护切换能力，但网络流量和拥塞控制能力差；

（3）不能像 IP over ATM 那样提供较好的故障链路和交换机恢复能力，较难保障服务质量（QoS）。

（4）仅对 IP 业务提供良好的支持，不适于多业务平台，可扩展性不理想，只有业务分级，而无业务质量分级，尚不支持 VPN 和电路仿真。

3．IP over DWDM（POW）

IP over WDM，也称光因特网，是 IP 与 DWDM 技术相结合的标志。首先在发送端对不同波长的光信号进行复用，然后将复用信号送入一根光纤中传输，在接收端再利用解复用器将各不同波长的光信号分开，送入相应的终端，从而实现 IP 数据报在多波长光路上的传输。

IP over WDM 的帧结构有 SDH 帧格式和千兆位以太网帧格式两种。

支持 IP over WDM 技术的协议、标准、技术和草案主要有：

（1）DWDM（密集波分复用）

一般峰值波长在 1～9nm 量级的 WDM 系统称为 DWDM。在此系统中，每一种波长的光信号都称为一个传输通道。每个通道都可以是一路 155Mbps、622Mbps、2.5Gbps 甚至 10Gbps 的 ATM、SDH 或千兆位以太网信号等。

DWDM 提供了接口的协议和速率的无关性，在一条光纤上，可以同时支持 ATM、SDH 和千兆位以太网，保护了已有投资，并提供了极大的灵活性。

（2）SDH 与千兆位以太网帧格式比较

SDH 帧格式下报头载有信令和足够的网络管理信息，便于网络管理。但相较而言，在路由器接口上针对 SDH 帧的拆装分割比较耗时，影响网络吞吐量和性能。

在局域网中主要采用千兆位以太网帧结构，此种格式下报头包含的网络状态信息不多，但由于没有使用一些造价高昂的再生设备，因而成本相对较低。由于使用的是“异步”协议，对抖动和时延不那么敏感。同时由于与主机的帧结构相同，因而在路由器接口上下需要对帧进行拆装分割（SAR）操作和为了使数据帧和传输帧同步的比特塞入操作。

IP over DWDM 的优点：

① 简化了层次，减少了网络设备和功能重叠，从而减轻了网络管理复杂程度；

② 可充分利用光纤的带宽资源，极大地提高了带宽和相对传输速率；

③ 对传输码率、数据格式及调制方式透明，可以传送不同码率的 ATM、SDH/SONET 和千兆位以太网业务，具有较好的各种通信网络兼容能力和可扩展能力。

IP over DWDM 的缺点：

① DWDM 极大的带宽与现有 IP 路由器有限的处理能力非常不匹配；

② 如果网络中没有 SDH 设备，IP 数据包就再也不能从每一个 SDH 帧中所包含的信头中找出故障所在，相应地，管理功能将被削弱；

③ 技术还不十分成熟，波长标准化还没有实现，一般取 193.1THz 为参考频率，间隔取 100GHz；

④ 常见的网络拓扑结构还是点对点的，还没有形成“光网”。

4.3.2　ATM 网络技术

从网络通信的角度，数据传输实际上涉及传输、复用、交换、终端等几部分。除终端以外的传输、复用和交换三个部分合起来统称为传递方式（也叫转移模式）。目前应用的传递方式可分为两种。①同步传递方式（Synchronous Transfer Mode，STM）：主要特征是采用时分复用，各路信号都按一定时间间隔周期性出现，接收端可根据时间（或位置）识别每路信号。②异步传递方式（Asynchronous Transfer Mode，ATM）：采用统计时分复用，各路信号不按照一定时间间隔周期性地出现，接收端要根据标志识别每路信号。

ATM 早期在许多主干网中得到应用，100Mbps 的快速以太网和千兆位等高速以太网推向市场后，ATM 在高速主干网的应用受到削弱，现在在电信、邮政的主干网段还有部分使用。它主要以光纤为传输介质，提供以太网 RJ45 接口和光纤接口两种接口与不同类型的物理网络实现互联互通。

1．ATM 基本概念

异步传递方式（ATM）就是建立在电路交换和分组交换的基础上的一种面向连接的快速分组交换技术。ATM 不但是数据链路层技术，可以运行在不同的物理介质上，还具有完整的网络层和传输层的各种特性，如寻址、路由及流控。

它采用定长分组作为传输和交换单位。在 ATM 中这种定长分组叫作信元（cell），包含同一用户数据的信元不需要在传输链路上周期性地出现。采用统计时分复用技术，根据标志识别每路信号，因此这种传递模式是异步的。

ATM 的主要优点如下。

（1）选择固定长度的短信元作为信息传输单位，有利于宽带高速交换。信元长度为 53 字节，其首部（可简称为信头）为 5 字节。长度固定的首部可使 ATM 交换机的功能尽量简化，只用硬件电路就可以对信元进行处理，因而缩短了每个信元的处理时间。在传输实时语音或视频业务时，短的信元有利于减小时延，也节约了节点交换机为存储信元所需的存储空间。

（2）能支持不同速率的各种业务。ATM 允许终端有足够多比特时就去利用信道，从而取得灵活的带宽共享。来自各终端的数字流在链路控制器中形成完整的信元后，即按先到先服务

的规则，经统计复用器，以统一的传输速率将信元插入一个空闲时隙内。链路控制器调节信息源进网的速率。不同类型的服务都可复用在一起，高速率信源占有较多的时隙。交换设备只需按网络最大速率来设置，它与用户设备的特性无关。

（3）所有信息在最低层都以面向连接的方式传送，保持了电路交换在保证实时性和服务质量方面的优点。ATM 既可工作于确定方式（即承载某种业务的信元基本上周期性地出现），以支持实时型业务；也可以工作于统计方式（即信元不规则地出现），以支持突发型业务。

（4）ATM 使用光纤信道传输。由于光纤信道的误码率极低，且容量很大，因此在 ATM 网内不必在数据链路层进行差错控制和流量控制（放在高层处理），因而明显提高了信元的传送速率。

ATM 的一个明显缺点就是信元首部的开销太大，即 5 字节的信元首部在整个 53 字节的信元中所占的比例相当大。

一个 ATM 网络包括两种网络元素，即 ATM 端点和 ATM 交换机。ATM 端点又称为 ATM 端系统，即在 ATM 网络中能够产生或接收信元的源站或目的站。ATM 端点通过点到点链路与 ATM 交换机相连。ATM 交换机是应用于 ATM 网络的交换机产品，也就是一个快速分组交换机（交换容量高达数百 Gbps），使得信元从某个输入端口交换到另外一个输出端口。由于 ATM 标准并不对 ATM 交换机的具体交换结构做出规定，因此现在已经出现了多种类型的 ATM 交换结构。例如 ADSL 宽带接入方式，如果采用 PPPoA 协议，在局端（ISP 端）就需要配置 ATM 交换机；同样，有线电视的互联网接入在局端也采用 ATM 交换机。

2．ATM 的协议参考模型

ATM 的协议参考模型如图 4-15 所示。

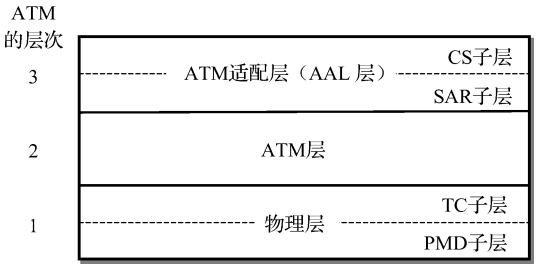


图 4-15　ATM 的协议参考模型

ATM 的协议参考模型共有三层，大体上与 OSI 的最低两层相当（无法严格对应）。靠下面的是物理媒体相关（Physical Medium Dependent）子层，即 PMD 子层。PMD 子层的上面是传输汇聚（Transmission Convergence，TC）子层。

（1）PMD 子层

PMD 子层负责在物理媒体上正确传输和接收比特流。它只完成和媒体相关的功能，如线路编码和解码、比特定时及光电转换等。对不同的传输媒体，PMD 子层是不同的。可供使用的传输媒体有铜线（UTP 或 STP）、同轴电缆、光纤（单模或多模）或无线信道等。

（2）TC 子层

TC 子层实现信元流和比特流的转换，包括速率适配（空闲信元的插入）、信元定界与同步、传输帧的产生与恢复等。在发送时，TC 子层将上面的 ATM 层递交下来的信元流转换成比特流，

再递交给下面的 PMD 子层。在接收时，TC 子层将 PMD 子层递交上来的比特流转换成信元流，标记出每一个信元的开始和结束，再递交给 ATM 层。TC 子层的存在使得 ATM 层与传输媒体完全无关。ATM 物理层中的 TC 子层的许多功能类似于 OSI 模型的数据链路层。典型的 TC 子层就是统一线路复接、传输及交换功能于一体的同步光网络/同步数字体系的 SONET/SDH。

（3）ATM 层

ATM 层主要完成交换和复用功能，与传送 ATM 信元的物理媒体或物理层无关。每个 ATM 连接都用信元首部中的两级标号来识别。第一级标号是虚通路标识（Virtual Channel Identifier，VCI），第二级标号是虚通道标识符（Virtual Path Identifier，VPI）。一个虚通路 VC 是在两个或两个以上的端点之间的一个运送 ATM 信元的通信通路。

一个虚通道 VP 包含有许多相同端点的虚通路，而这许多虚通路都使用同一个虚通道标识符（VPI）。在一个给定的接口，复用在一条链路上的许多不同的虚通道，用它们的虚通道标识符（VPI）来识别；复用在一个虚通道中的不同的虚通路，用它们的虚通路标识符（VCI）来识别。图 4-16 表示了使用 VPI 和 VCI 来标识 VP 和 VC 的方法。

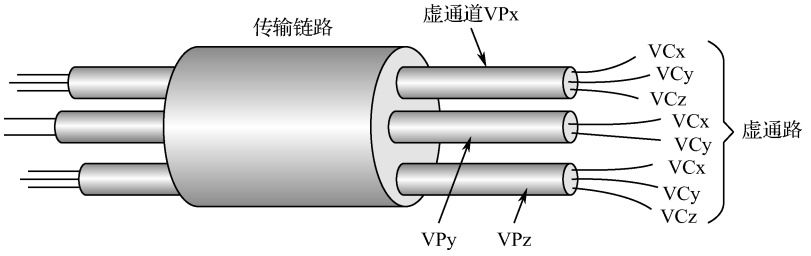


图 4-16　ATM 连接的标识符 VCI 和 VPI

在一个给定的接口上，属于两个不同的 VP 的两个 VC 可以具有相同的 VCI。如图 4-16 中所示的三个不同的虚通道 VP 都可以使用相同的虚通路标识符 VCx 或 VCy。因此，要同时使用 VPI 和 VCI 两个参数才能完全识别一个虚通路 VC。

ATM 层的功能是：信元的复用与分用；信元的 VPI/VCI 转换（就是将一个入信元的 VPI/VCI 转换成新的数值）；信元首部的产生与提取；流量控制。

（4）ATM 适配层

ATM 传送和交换的是 53 字节固定长度的信元。但是上层的应用程序向下层传递的并不是 53 字节长的信元。因此当 IP 数据报需要在 ATM 网络上传送时，就需要有一个接口，它能够将 IP 数据报装入一个个 ATM 信元，然后在 ATM 网络中传送。这个接口就是在 ATM 层上面的 ATM 适配层，记为 AAL（ATM Adaptation Layer）。AAL 层向上层提供各种不同的服务。图 4-17 表示不同信源发出的信号（语音、视频、数据等）通过 AAL 层后都变成了固定长度的数据块（48 字节长），然后交给 ATM 层，加上 5 字节的首部后变成 53 字节的信元。

ITU-T 规定了 AAL 向上提供的服务：将用户的应用数据单元（ADU）划分为信元或将信元重装成为应用数据单元（ADU）；对比特差错进行检测和处理；处理丢失和错误交付的信元；流量控制和定时控制。

AAL 层的功能只能驻留在 ATM 端点之中，而在 ATM 交换机中只有物理层和 ATM 层，如图 4-18 所示。不同的物理链路可采用不同的物理传输媒体。

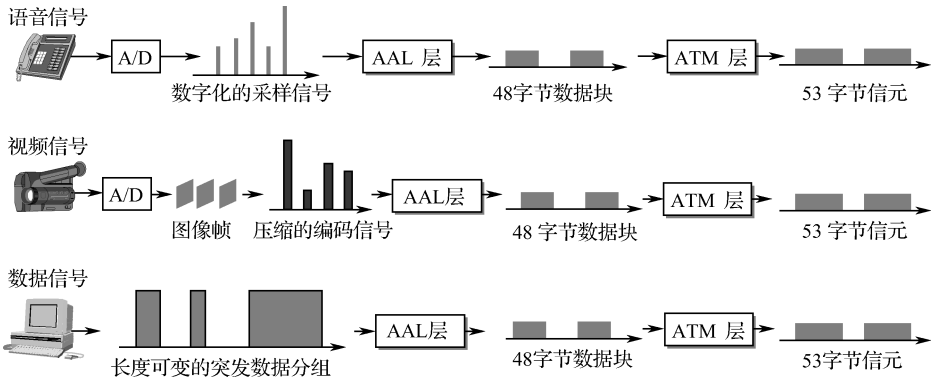


图 4-17　ATM 适配示意图

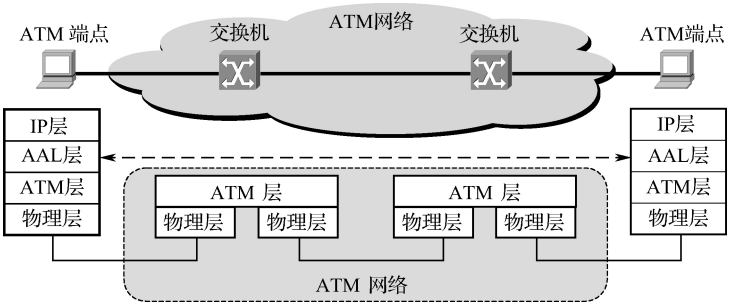


图 4-18　AAL 层只能驻留在 ATM 端点之中

最简单的 ATM 网络可以只有一个 ATM 交换机，通过一些点到点链路与各 ATM 端点相连。从图 4-18 可见，当孤立地观察一个 ATM 网络时，ATM 网络像一个广域网，因为它可以覆盖很大的地理范围，有自己网络的硬件地址和进行信元转发的结点交换机，并且向上提供虚电路服务。不过从 IP 层来看，整个 ATM 网络又相当于两个 IP 节点之间的一条数据链路。从这个角度看，整个 ATM 网络又好像是处在数据链路层。

3．在 ATM 上传输 IP 数据包

IPOA（IP over ATM）是在 ATM-LAN 上传送 IP 数据包的一种技术。它规定了利用 ATM 网络在 ATM 终端间建立连接，特别是建立交换型虚连接（Switched Virtual Circuit，SVC）进行 IP 数据通信的规范。

在 ATM-LAN 中，ATM 网络可看作一个单一的、独立的局域网，网中的所有计算机被叫作 LIS（Logical IP Subnet），一个 LIS 内的计算机共享一个 IP 网络地址（IP 子网地址），LIS 内部的计算机可以互相直接通信，但是当一个 LIS 内的计算机要和其他 LIS 或网络中的计算机通信时，必须经过两个互连的 LIS 路由器，很明显，LIS 的特性与传统 IP 子网相似。

类似以太网，IP 数据包在 ATM 网络上传输也必须进行 IP 地址绑定，ATM 给网内每一个计算机分配 ATM 物理地址，当建立虚连接时必须使用这个物理地址，但由于 ATM 硬件不支持广播，所以，IP 无法使用传统的 ARP 将其地址绑定到 ATM 地址。在 ATM 网络中，每一个 LIS 配置至少一个 ATMARP Server 以完成地址绑定工作。

用 ATM 来支持 IP 业务有两个必须解决的问题：其一是 ATM 的通信方式是面向连接的，而 IP 是不面向连接的，要在一个面向连接的网上承载一个不面向连接的业务，有很多问题需

要解决，如呼叫建立时间、连接持续期等；其二是 ATM 是以 ATM 地址寻址的，IP 通信是以 IP 地址寻址的，在 IP 网上端到端是以 IP 寻址的，而传送 IP 包的 ATM 网是以 ATM 地址寻址的，IP 地址和 ATM 地址之间的映射是一个难题。

所以 IPOA 有两个主要功能：地址解析和数据封装。

地址解析就是完成地址绑定功能。对于 PVC（Permanent Virtual Circuit）来说，因为 PVC 是由管理员手动配置的，因此一个主机可能只知道 PVC 的 VPI/VCI 标识，而不知道远地主机的 IP 地址和 ATM 地址，这就需要 IP 解析机制能够识别连接在一条 PVC 上的远地计算机；对于 SVC 来说，地址解析更加复杂，需要两级地址解析过程。首先，当需要建立 SVC 时，必须把目的端的 IP 地址解析成 ATM 地址；其次，当在一条已有的 SVC 上传输数据包时，目的端的 IP 地址必须映射成 SVC 的 VPI/VCI 标识。

对于 IP 数据包，有两种封装形式：一种是一条 VC 仅用于传输一种特定的协议数据（如 IP 数据和 ARP 数据），传输效率很高；另外一种就是使用同一条 VC 传输多种协议数据，这样必须给数据加上类型字段，IPOA 中使用默认的 LLC/SNAP 封装标明数据类型信息。

IPOA 在 TCP/IP 协议栈中的位置：ATM 网络是面向连接的，TCP/IP 只是将其作为像以太网一样的另一种物理网络来看待。从 TCP/IP 的协议体系结构来看，除了要建立虚连接之外，IPOA 与网络接口层完成的功能类似，即完成 IP 地址到硬件地址（ATM 地址）的映射过程，封装并发送输出的数据分组，接收输入的数据分组并将其发送到对应的模块。当然，除了以上功能之外，网络接口还负责与硬件通信（设备驱动程序也属于网络接口层）。

IPOA 最大的优点就是其利用了 ATM 网络的 QoS，可以支持多媒体业务，它在网络层将局域网接入 ATM 网络，既提高了网络带宽，又提升了网络的性能，适合用在企业网、校园网等小网中。但 IPOA 也存在一些缺点，如 IPOA 网络体系结构复杂、传输效率低、开销损失大，不支持广播和组播业务，不适合于大网结构等。由于 IPOA 技术进展缓慢，特别是在 MPLS 没有提出和标准化之前，ATM 网不能满足带宽 IP 的应用需求，导致了 IP over SDH 技术的出现。

4.3.3　SDH 网络技术

SDH（Synchronous Digital Hierarchy，同步数字体系）是一种将复接、线路传输及交换功能融为一体并由统一网络管理系统操作的综合信息传送网络，是美国贝尔通信技术研究所提出的同步光网络（SONET）。国际电话电报咨询委员会（CCITT）（现 ITU-T）于 1988 年接受了 SONET 概念并重新命名为 SDH，广泛应用于主干网和接入网中，成为不仅适用于光纤也适用于微波和卫星传输的通用技术体制。它可实现网络有效管理、实时业务监控、动态网络维护、不同厂商设备间的互通等多项功能，能大大提高网络资源利用率、降低管理及维护费用、实现灵活可靠和高效的网络运行与维护。

1．SDH 的基本传输原理

SDH 网是一个时分复用系统，对网络节点接口做了统一的规范。规范的内容有数字信号速率等级、帧结构、复接方法、线路接口、监控管理等，这就使 SDH 设备容易实现多厂家互连，也就是说在同一传输线路上可以安装不同厂家的设备，体现了横向兼容性。

SDH 体制有一套标准的信息结构等级，即有一套标准的速率等级。基本的信号传输结构等级是同步传输模块——STM-1，相应的速率是 155Mbps。高等级的数字信号系列如 622Mbps

（STM-4）、2.5Gbps（STM-16）等，是通过将低速率等级的信息模块（如 STM−1）通过字节间插同步复接而成，复接的个数是 4 的倍数，如 STM−4=4×STM−1，STM−16=4×STM−4。

字节间插方式使低速 SDH 信号在高速 SDH 信号的帧中的位置是固定的、有规律的，也就是说是可预见的。这样就能从高速 SDH 信号如 2.5Gbps（STM−16）中直接分/插出低速 SDH 信号，如 155Mbps（STM−1），从而简化了信号的复接和分接，使 SDH 体制特别适合于高速大容量的光纤通信系统。

2．SDH 的特点

SDH 之所以能够快速发展与它自身的特点是分不开的，其具体特点如下。

（1）SDH 传输系统在国际上有统一的帧结构、数字传输标准速率和标准的光路接口，形成了全球统一的数字传输体制标准，使网络管理系统互通，因此有很好的横向兼容性和网络可靠性。

（2）能统一形成网络管理系统，为网络的自动化、智能化，提高信道的利用率及降低网络维管费和生存能力起到了积极作用。

（3）SDH 有多种网络拓扑结构，具有传输和交换能力，组网非常灵活，能运行管理和自动配置，优化网络性能。

（4）SDH 并不专属于某种传输介质，它可用于双绞线、同轴电缆，但 SDH 用于传输高数据率则需用光纤。这一特点表明，SDH 既适合用作干线通道，也可用作支线通道。例如，我国的国家与省级有线电视干线网就采用 SDH，而且它也便于与光纤电缆混合网（HFC）兼容。

（5）从 OSI 模型的观点来看，SDH 属于其底层的物理层，并未对其高层有严格的限制，便于在 SDH 上采用各种网络技术，支持 ATM 或 IP 传输。例如，只要 SDH 的帧有空位置，就可以将 ATM 信元“异步插入”到同步的 SDH 比特流中，从而把 SDH/SONET 作为 ATM 的一种物理层。

3．SDH 的应用

SDH 在广域网和专用网中得到了巨大发展。电信、联通、广电等电信运营商都已经大规模建设了基于 SDH 的骨干光传输网络。利用大容量的 SDH 环路承载 IP 业务、ATM 业务或直接以租用电路的方式出租给企、事业单位。一些大型的专用网络也采用了 SDH 技术，架设系统内部的 SDH 光环路，以承载各种业务。

SDH 的安全性也优于 VPN 等方式。在政府机关和军事领域，SDH 租用线路得到了广泛应用。一般来说，SDH 可提供 E1、E3、STM-1 或 STM-4 等接口，完全可以满足并保证各种带宽要求。

4.3.4 DDN 网络技术

数字数据网（DDN）是采用数字信道来传输数据信息的数据传输网。数字信道包括用户到网络的连接线路，即用户环路的传输也应该是数字的。DDN 一般用于向用户提供专用的数字数据传输信道，或提供将用户接入公用数据交换网的接入信道，也可以为公用数据交换网提供交换节点间用的数据传输信道。

DDN 是利用数字信道为用户提供语音、数据、图像信号的半永久连接电路的传输网路。

半永久性连接是指 DDN 所提供的信道是非交换性的，用户之间的通信通常是固定的。一旦用户提出改变的申请，由网络管理人员或在网络允许的情况下由用户自己对传输速率、传输数据的目的地及与传输路由进行修改，但这种修改不是经常性的，所以称为半永久性连接或半固定交叉连接。它克服了数据通信专用链路永久连接的不灵活性，以及以 X.25 建议为核心的分组交换网络的处理速度慢、传输时延大等缺点。

1．DDN 的优点

DDN 向用户提供端到端的数字型传输信道，它与在模拟信道上采用调制解调器（MODEM）来实现的数据传输相比，有下列特点：

（1）传输差错率（误比特率）低

一般数字信道的正常误码率在 10^{-6} 以下，而模拟信道较难达到。

（2）信道利用率高

一条 PCM 数字话路的典型传输速率为 64Kbps。通过复用可以传输多路 19.2Kbps 或 9.6Kbps 或更低速率的数据信号。

（3）无需 MODEM

与用户的数据终端设备相连的数据电路终接设备（DCE）一般只是一种功能较简单的通常称作数据服务单元（DSU）或数据终接单元（DTU）的基带传输装置，或者直接是一个复用器相应的接口单元。

（4）要求全网的时钟系统保持同步

DDN 要求全网的时钟系统必须保持同步，否则，在实现电路的转接、复接和分接时就会遇到较大的困难。

2．DDN 的网络组成

DDN 由用户环路、DDN 节点、数字信道和网络控制管理中心组成，其网络组成结构框图如 4-19 所示。用户环路又称用户接入系统，通常包括用户设备、用户线和用户接入单元。用户设备通常是数据终端设备（DTE）（如电话机、传真机、个人计算机及用户自选的其他用户终端设备）。目前用户线一般采用市话电缆的双绞线。用户接入单元可由多种设备组成，对目前的数据通信而言，通常是基带型或频带型单路或多路复用传输设备。

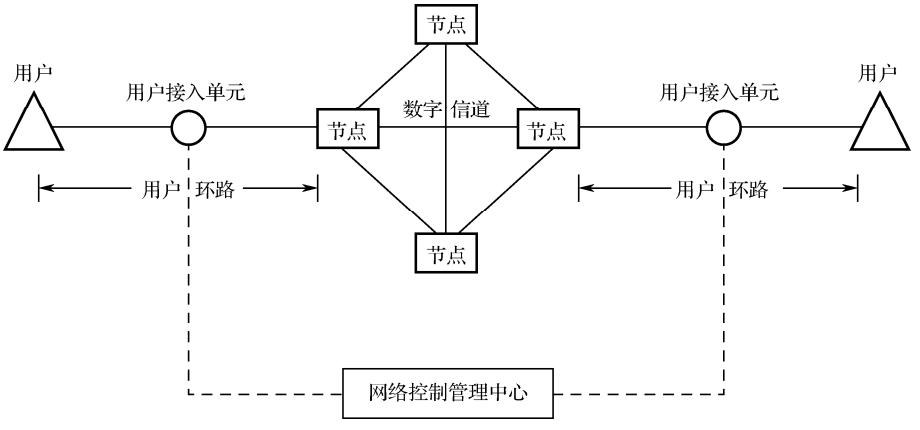


图 4-19　DDN 网络组成结构框图

从组网功能区分，DDN 节点可分为用户节点、接入节点和 E1 节点。从网络结构区分，DDN 节点可分为一级干线网节点、二级干线网节点及本地网节点。

（1）用户节点

用户节点主要为 DDN 用户入网提供接口并进行必要的协议转换，这包括小容量时分复用设备及 LAN 通过帧中继互连的桥接器/路由器等。小容量时分复用设备也可包括压缩语音/G3 传真用户接口。

（2）接入节点

接入节点主要为 DDN 各类业务提供接入功能，主要包括 *N*×64Kbps（*N*=1～31），2048Kbps 数字信道的接口；*N*×64Kbps 的复用；小于 64Kbps 的子速率复用和交叉连接；帧中继业务用户的接入和本地帧中继功能；压缩语音/G3 传真用户的接入功能。

（3）E1 节点

E1 节点用于网上的骨干节点，执行网络业务的转接功能。E1 节点主要提供 2048Kbps（E1）接口，对 *N*×64Kbps 进行复用和交叉连接，以收集来自不同方向的 *N*×64Kbps 电路，并把它们归并到适当方向的 E1 输出，或直接接到 E1 进行交叉连接。

（4）枢纽节点

枢纽节点用于 DDN 的一级干线网和各二级干线网。它与各节点通过数字信道相连，容量大，因而故障时影响面大。在设置枢纽节点时，可考虑备用数字信道的设备，同时合理地组织各节点互连，充分发挥其效率。

网络控制管理是保证全网正常运行、发挥其最佳性能效益的重要手段。网络控制管理一般应具有以下功能：①用户接入管理（包括安全管理）；②网络结构和业务的配置；③网络资源与路由管理；④实时监视网络运行；⑤维护、告警、测量和故障区段定位；⑥网络运行数据的收集与统计；⑦计费信息的收集与报告。

3．DDN 的网络结构

DDN 网按组建、运营和管理维护的责任区域来划分网络等级，可分为本地网和干线网，干线网又分为一级干线网、二级干线网。一级干线网由各省、市、自治区的节点组成，它提供省间长途 DDN 业务；二级干线网由省内节点组成，它提供本省内长途和出入省的 DDN 业务；不同等级的网络主要用 2048Kbps 数字信道互连，也可用 *N*×64Kbps 数字信道互连。

4．DDN 的互连

用户网络与 DDN 互连方式：DDN 作为一种数据业务的承载网络，不仅可以实现用户终端的接入，还可以是局域网、专用数字数据网、分组交换网、用户交换机及其他用户网络。局域网可通过路由器等设备与 DDN 互连，其互连接口采用 ITU-TG.703 或 V.35、X.21 标准，这种连接本质上是局域网与局域网的互连。

DDN 是流行的专用线路数据网，通过电信运营商为通信双方建立永久性专用线路。军事专用 DDN 覆盖的地理区域有限，结构简单，适合有固定速率的高通信量网络环境。专用 DDN 与公用 DDN 可以采用 V.24、V.35、X.21 标准互连，也可以采用 G.703 2048Kbps 标准互连。具体互连时对信道的传输速率、接口标准及所经路由等方面的要求可按专用 DDN 需要确定。

4.4 VPN 技术与 MPLS 协议

4.4.1 VPN 虚拟专用网技术

虚拟专用网络（Virtual Private Network，VPN）是在公共通信基础设施上构建的虚拟专用网或私有网，如图 4-20 所示。它对位于不同地方的两个或多个内部网络采用特殊加密的通信协议，建立一条专有通信线路，通过对网络数据进行封包和加密，在公网上传输私有数据，使得各内部网能够相互通信，同时保证私有网络的安全性。

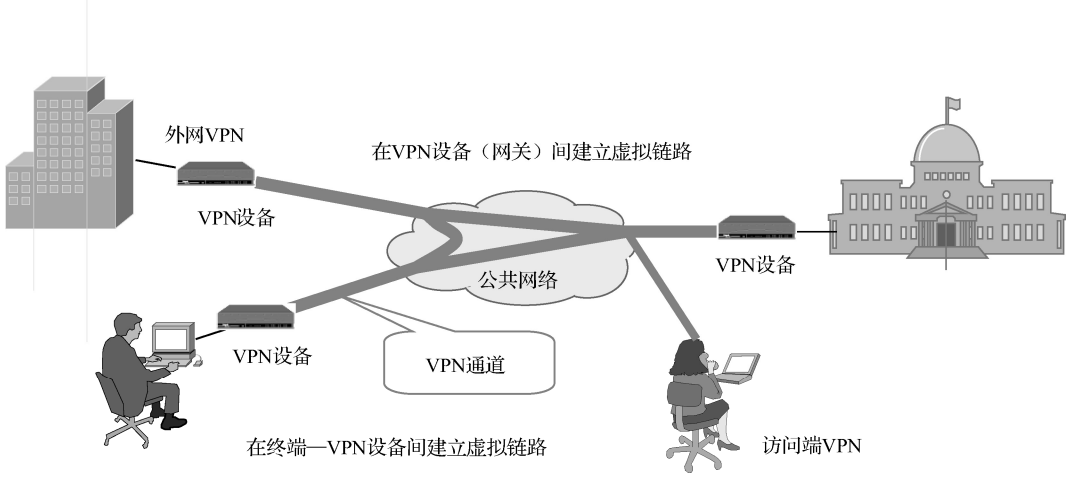


图 4-20　虚拟专用网示意图

VPN 是一种逻辑上的网络，不是真正的专用网络，却能实现专用网络的功能。它兼备了公网的便捷性和专用网的安全性，实现了利用公网通过加密等手段来实现单位组织的“专用网”。需要进行机密数据传输的两个端点均连接在公共通信网上，当需要进行机密数据传输时，通过端点上的 VPN 设备在公共网上建立一条虚拟的专用网络通道，并且所有数据均经过加密后再在网上传输，这样就保证了机密数据的安全传输。VPN 既可验证数据发送端，保证数据传输的完整性和机密性，还可避免传输信息被窃取或内部网络被攻击，因此在军事网络中常有应用。

1．VPN 的技术原理

VPN 技术是指支持在公共通信基础设施上构成虚拟专用连接或虚拟专用网络的技术。这些技术包括配置管理技术、隧道技术、协议封装技术和密码技术等。这些技术可应用在 TCP/IP 协议层的数据链路层、IP 层、TCP 层和应用层。

（1）VPN 封装技术：在公共网络上建立一个通信隧道，利用公共网络的可路由地址封装内部网络的 IP 地址，实现异地网络的互通。本来不能通信的两个分处异地的局域网，通过出口处的 IP 地址封装，实现局域网对局域网的通信。

（2）协议加密：VPN 的加密技术和封装技术是一样的。既然能够把数据封装，自然也可以把数据变换，只要到达目的地时能够把数据恢复成原来的样子即可，加密工作在互联网出口的 VPN 网关上完成。

（3）数据认证：仅有加密技术是不够的，还需要引入数据防篡改机制，一旦数据被非法修改，必须能够很快识别出来。VPN 使用 MD5 或 EDS 算法计算报文特征，报文还原以后，就会检查这个特征码，查看是否匹配，以此来证明数据传输过程是否被篡改。

（4）身份认证：常见的 VPN 身份认证包括预共享密钥，通信双方实现约定加密解密的密码，直接通信就可以了。能够通信就是可信任用户，不能通信就是非授权用户。

2．VPN 的分类

（1）按 VPN 的协议分类

VPN 的隧道协议主要有三种：PPTP、L2TP 和 IPSec。PPTP 和 L2TP 工作在 OSI 模型的第二层，又称第二层隧道协议，IPSec 是第三层隧道协议，也是最常见的协议。L2TP 和 IPSec 配合使用是目前性能最好、应用最广泛的。

（2）按所用的设备类型分类

针对不同的需求，VPN 网络设备主要有交换机、路由器和防火墙。

路由器式 VPN：VPN 较容易部署，通常只需升级路由器软件、添加 VPN 服务。

交换机式 VPN：主要应用于连接用户较少的 VPN 网络中，多为 3Com 公司生产。

防火墙式 VPN：基于防火墙的 VPN 最为常见，许多厂商都提供这种配置类型。其产品在不同的平台都能有效使用，但需确认操作系统的安全。

3．VPN 的关键技术

（1）隧道技术

隧道技术是指包括数据封装、传输和解包在内的全过程，创建隧道的客户机和服务器双方必须使用相同的隧道协议。VPN 采用隧道技术向用户提供无缝的、安全的、端到端的连接服务，以确保信息资源的安全。

所谓隧道，实质上是一种封装，就是将一种协议（协议 X）封装在另一种协议（协议 Y）中传输，从而实现协议 X 对公用网络的透明性。这里协议 X 称为被封装协议，协议 Y 称为封装协议，封装时一般还要加上特定的隧道控制信息，因此隧道协议的一般形式为（协议 Y（隧道头（协议 X））。隧道解决了专网与公网的兼容问题，其优点是能够隐藏发送者、接收者的 IP 地址及其他协议信息。在公用网络传输过程中，只有 VPN 端口或网关的 IP 地址暴露在外边。

第二层隧道和第三层隧道的本质区别在于：用户的 IP 数据包被封装在不同的数据包中在隧道中传输。第二层隧道协议建立在点对点数据链路层协议（PPP）的基础上，充分利用了 PPP 支持多协议的特点，由 PPP 帧构成数据包，再装入 PPTP 和 L2TP 等隧道协议，实现远程访问虚拟专用网，如图 4-21 所示。第三层隧道协议把各种网络协议直接装入 IPSec、GRE 等隧道协议中，形成的数据包依靠网络层 IP 进行传输。无论从可扩充性，还是安全性、可靠性方面，第三层隧道协议均优于第二层隧道协议。IPSec 是目前实现 VPN 功能的最佳选择，适合各个局域网之间组建内部虚拟专用网。

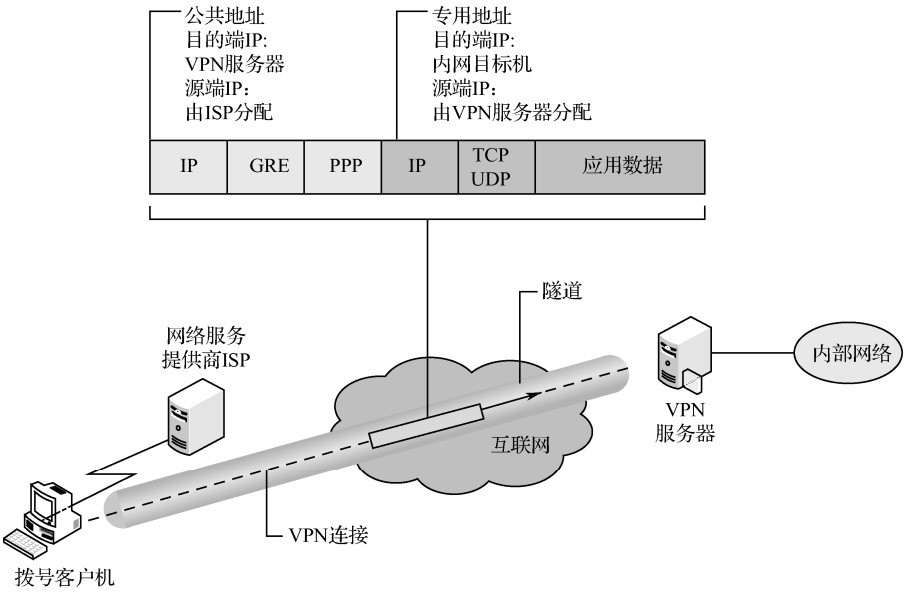


图 4-21　PPTP 数据包中的公共地址和专用地址

（2）加解密、认证技术

加解密、认证技术是 VPN 的另一核心技术。为了保证数据在传输过程中的安全性，不被非法用户窃取或篡改，一般都在传输之前进行加密，接收方再对其进行解密。

密码技术是保证数据安全传输的关键技术，以密钥为标准，可将密码系统分为单钥密码（又称为对称密码或私钥密码）和双钥密码（又称为非对称密码或公钥密码）。单钥密码的特点是加密和解密都使用同一个密钥，加解密速度快，如 DES、3DES 等。双钥密码体制下，加密密钥与解密密钥不同，加密密钥公开，而解密密钥保密，比单钥体制算法复杂且加解密速度慢。

认证技术可以防止来自第三方的主动攻击。一般用户和设备双方在交换数据前先核对证书，如果准确无误，双方才开始交换数据。用户身份认证最常用的技术是用户名与密码方式。而设备认证则需要依赖由 CA 所颁发的电子证书。

（3）密钥管理技术

密钥管理的主要任务是保证在开放的网络环境中安全地传递密钥，而不被窃取。目前密钥管理协议包括 ISAKMP、SKIP、MKAP 等。

（4）访问控制技术

虚拟专用网可以灵活配置不同用户对不同主机或服务器的访问权限。访问控制策略可以细分为选择性访问控制和强制性访问控制。选择性访问控制基于主体或主体所在组的身份，一般被内置于许多操作系统当中，强制性访问控制基于被访问信息的敏感性。

4．VPN 的优点

（1）降低成本：通过公用网来建立 VPN 与建立 DDN 等专线方式相比，可节省大量费用。

（2）伸缩性高：无须建立租用线路或帧中继线路，只需双方配置安全连接信息即可。当不再需要连网时，也很容易拆除连接。

（3）容易扩展：如果想扩大 VPN 的容量和覆盖范围，只需改变一些配置或增加几台设备。

（4）安全控制主动权：可以利用公网或在局域网内部自己组建 VPN，并自己负责用户的查验、访问权、网络地址、安全性和网络变化管理等重要工作。

（5）全方位的安全保护：VPN 不仅能在网络与网络之间建立专用通道，保护网关与网关之间信息传输的安全，而且能在子网内部的用户与网关之间、移动办公用户和网关之间、用户与用户之间建立安全通道，建立全方位的安全保护，保证网络安全。

5．VPN 的应用

VPN 专网是军事信息地面网络的重要组成部分，主要由传输控制设备、路由器、保密机和既有的军事公共信息网组成。例如，A、B 为不同地域的两军事系统局域网络，各网内均使用私有的 IP 地址（10.0.1.0/24 和 10.0.2.0/24），对外不能相互访问，为了在 A、B 之间实现内部军事信息资源共享，则需要在局域网 A、B 的网关路由器 R1、R2 上安装基于 IPSec 的 VPN 服务器，同时在两端的路由器上建立 VPN 连接客户端，并设置对方局域网的静态路由，使局域网 A、B 共享一个证书机构 CA 和安全策略服务器，如图 4-22 所示。

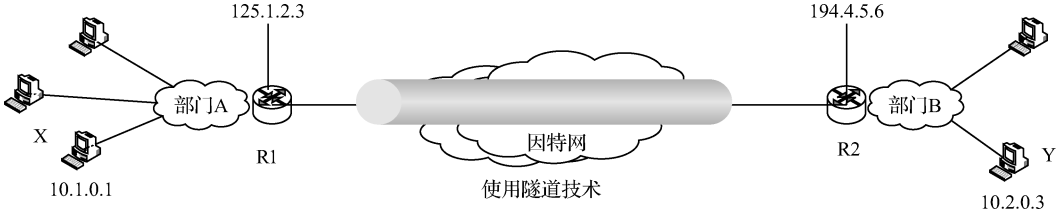


图 4-22　VPN 应用

这样，当 A 网内的某一计算机 X（10.1.0.1）需要访问 B 网内的某一计算机 Y（10.2.0.3）时，路由器 R1（125.1.2.3）就作为 VPN 的客户端向 VPN 服务器 R2（194.4.5.6）发出呼叫连接请求，在用户的身份得到认证后，VPN 服务器 R2 就响应连接请求，同时，R2 以客户端的身份向 VPN 服务器 R1 发出连接请求。当两个连接建立之后，R1 和 R2 之间就拥有了一条进行数据传输的专用虚拟通道，A、B 两局域网就可以通过各自路由器上的静态路由访问对方。由于隧道中传输的是加密数据，因此，不必担心内部的重要数据在传输的过程中被其他用户窃取，从而使得内部的信息和资源得到保护。

4.4.2　MPLS 交换协议

多协议标签交换协议（Multi-Protocol Label Switching，MPLS）是一种用于快速数据包交换和路由的体系。出发点是把路由器和 ATM 交换机融为一体，具有管理各种不同形式通信流的机制，为网络数据流量提供目标、路由、转发和交换等能力，能够解决流量管理、虚拟专用网 VPN、服务质量（QoS）管理等网路问题，可简化网络并提高 IP 包的传送速度，是 L3 Switching（三层交换）技术的国际标准。

MPLS 技术是 ATM 和 IP 的集成模型，兼容传统的 IP 路由协议，将 IP 地址映射为简单的具有固定长度的标签，用于不同的包转发和包交换。它是现有 IP、ATM、帧中继、资源预留协议（RSVP）、开放最短路径优先（OSPF）等路由和交换协议的接口。

它首先将整个可能的分组集合划分为转发等价类（Forwarding Equivalence Class，FEC），使得转发处理方式或转发路径相同的 IP 分组归为一类；然后根据 LDP（Label Distribution Protocol，标记分布协议）在传统的第三层的报头前加上固定长度标签 Label（标记）；LDP 运行在由 Label 交换机（Label Switch Router，LSR）和 Label 边缘路由器（Eage LSR）组成的 MPLS 交换网络内，网内每个 MPLS 路由器都建立了类似于传统路由表的标签路由表。在转发数据报时，查找这些固定长度的标签路由表以快速转发数据报，而传统的路由表查找采用的是最长前缀匹配法。LDP 协议用来建立传统的路由表和标签路由间的对应关系，从而在 MPLS 路由器之间建立一条基于标签的数据报转发的快捷路径。MPLS 也可以使用开放最短路径优先协议（OSPF）建立快捷路径而不采用 LDP 协议。

MPLS 的基本工作过程：

（1）LDP 和传统路由协议（如 OSPF 等）一起，在各个 LSR 中为有业务需求的 FEC 建立路由表和标签映射表；

（2）入节点接收分组，完成第三层功能，判定分组所属的 FEC，并给分组加上标签，形成 MPLS 标签分组，转发到中间节点；

（3）中间节点根据分组上的标签及标签转发表进行转发，不对标签分组进行任何第三层处理；

（4）出节点去掉分组中的标签，继续进行后面的转发。

MPLS 交换网络既不运行 ATM 信元，也不运行 TCP/IP 包，网络内部进行的只是 Label 交换，具体就是依据 Label 对贴有标记的数据包进行交换。Label 交换机可以看作路由器和 ATM 交换机的结合体；Label 边缘路由器既支持 MPLS 也支持传统的 IP 路由网络技术。在 Label 交换网络的外围，传统的 IP 路由网络可以通过 Tag 边缘路由器接入作为骨干的 Label 交换网络。

由此可以看出，MPLS 并不是一种业务或应用，它实际上是一种隧道技术，也是一种集标签交换转发和网络层路由技术于一身的路由与交换技术平台。这个平台不仅支持多种高层协议与业务，而且在一定程度上可以保证信息传输的安全性。

基于 MPLS 的 VPN 一般由服务提供商核心路由器（P-Router）、服务提供商边界路由器（Provider Edge-Router，PE-Router）、用户边缘路由器（Customer Edge-Router，CE-Router）组成。P-Router 服务提供商核心路由器，快速标记交换用户数据。PE-Router 服务提供商边界路由器。一端与 CE-Router 直接相连，另一端与 P-Router 相连。PE-Router 判别相连的 CE-Router 属于哪一个 VPN，并为每个 VPN 维护一个路由表。PE-Router 将 IPv4 地址转换为 VPN-IPv4 地址，从而允许不同 VPN 之间的 IP 地址可以重叠。CE-Router 为用户边缘路由器，与 PE-Router 直接相连。

MPLS-VPN 的基本工作方式是采用三层技术，每一个 VPN 都具有独自的 VPN-ID，每个 VPN 用户只能与自己 VPN 网络中的成员进行通信，只有 VPN 的成员才有权进入该 VPN。

MPLS 在 21 世纪后得到了广泛应用，并导致 VPN 技术产生了质的变化。它保证了 VPN 极高的可扩展性，并为服务供应商和最终用户同时提供简单配置和可管理性。MPLS 同时可以提供跨越 IP 路由网络和 ATM 交换网络的 VPN，从而保护用户的现有投资。MPLS 技术还支持 RSVP（Resource Reservation Protocol，资源预留协议）协议，可以把 RSVP 指定的 QoS 要求映射到 MPLS 技术的 QoS 级别上，从而支持端到端的 QoS 保证。

4.5 路由器的使用

4.5.1 路由器的选购

1．路由器的分类

（1）按档次分

路由器分高、中和低档，各厂家划分标准并不完全一致，通常以背板交换能力为依据。

（2）按结构分

从结构上分，路由器可分为模块化结构与非模块化结构的。模块化结构可以灵活地配置路由器，以适应企业不断增加的业务需求；非模块化的路由器只能提供固定端口。通常中高端路由器为模块化结构的，低端路由器为非模块化结构的。

（3）按功能划分

从功能上划分，可将路由器分为核心层（骨干级）路由器，分发层（企业级）路由器和访问层（接入级）路由器。

骨干级路由器：骨干级路由器是实现企业级网络互连的关键设备，它数据吞吐量较大，非常重要。对骨干级路由器的基本性能要求是高速度和高可靠性。

企业级路由器：企业级或校园级路由器连接许多终端系统，连接对象较多，但系统相对简单，且数据流量较小，对这类路由器的要求是以尽量便宜的方法实现尽可能多的端点互连，同时要求能够支持不同的服务质量。

接入级路由器：接入级路由器主要应用于连接家庭或 ISP 内的小型群体。

（4）按应用划分

从应用上划分，路由器可分为通用路由器与专用路由器。一般所说的路由器皆为通用路由器。专用路由器通常为实现某种特定功能对路由器接口、硬件等做专门优化，如接入服务器用作接入拨号用户，增强 PSTN 接口及信令能力；VPN 路由器用于为远程 VPN 访问用户提供路由，它需要在隧道处理能力及硬件加密等方面具备特定的能力。

（5）按所处网络位置划分

如果按路由器所处的网络位置划分，则通常把路由器划分为边界路由器和中间节点路由器两类。边界路由器处于网络边缘，用于不同网络路由器的连接；而中间节点路由器则处于网络的中间，通常用于连接不同网络，起到数据转发的桥梁作用。

（6）按性能划分

从性能上分，路由器可分为线速路由器及非线速路由器。所谓线速路由器就是完全可以按传输介质带宽进行通畅传输，基本上没有间断和延时。通常线速路由器是高端路由器，具有非常高的端口带宽和数据转发能力，能以媒体速率转发数据包；中低端路由器是非线速路由器，但是一些新的宽带接入路由器也有线速转发能力。

2．路由器和交换机的区别

路由器产生于交换机之后，所以路由器与交换机也有一定的联系，并不是完全独立的两种设备。路由器主要克服了交换机不能路由转发数据包的不足。总的来说，路由器与交换机的主要区别体现在以下几个方面。

（1）工作层次不同

最初的交换机工作在 OSI/RM 开放体系结构的数据链路层，也就是第二层，而路由器一开始就设计工作在 OSI 模型的网络层。由于交换机工作在 OSI 的第二层（数据链路层），所以它的工作原理比较简单，而路由器工作在 OSI 的第三层（网络层），可以得到更多的协议信息，路由器可以做出更加智能的转发决策。

（2）数据转发所依据的对象不同

交换机利用物理地址或者说 MAC 地址来确定转发数据的目的地址；而路由器则利用不同网络的 ID 号（即 IP 地址）来确定数据转发的地址。IP 地址是在软件中实现的，描述的是设备所在的网络，有时这些第三层的地址也称为协议地址或网络地址。MAC 地址通常是硬件自带的，由网卡生产商来分配，而且已经固化到了网卡中，一般来说是不可更改的。而 IP 地址则通常由网络管理员或系统自动分配。

（3）路由器可以分割广播域

传统的交换机只能分割冲突域，不能分割广播域；而路由器可以分割广播域。由交换机连接的网段仍属于同一个广播域，广播数据包会在交换机连接的所有网段上传播，在某些情况下会导致通信拥挤和安全漏洞。连接到路由器上的网段会被分配成不同的广播域，广播数据不会穿过路由器。虽然第三层以上交换机具有 VLAN 功能，也可以分割广播域，但是各子广播域之间不能通信，它们之间的交流仍然需要路由器。

（4）路由器可以防止广播风暴

路由器提供了防火墙服务，它仅转发特定地址的数据包，不支持路由协议的数据包传送和未知目标网络的数据包传送，从而可以防止广播风暴。

3．路由器的选购

路由器最常用的指标有以下几个。

带宽（bandwidth）：链路的数据承载能力。

延迟（delay）：把数据包从源端送到目标端所需的时间。

负载（load）：在路由器或链路上的通信信息量。

可靠性（reliability）：网络中每条通信链路上的差错率。

跳数（hopcount）：数据包从源端到达目的端所必须通过的路由器个数。

滴答数（ticks）：数据链路延迟。

路由器的选购主要从以下几个方面考虑。

（1）路由器的管理方式

路由器最基本的管理方式是利用终端（如 Windows 系统所提供的超级终端）通过专用配置线连接到路由器的 Console 端口（配置端口）直接进行配置。因为新购买的路由器配置文件是空的，所以用户购买路由器以后一般都先使用此方式对路由器进行基本配置。但要对路由器进行全面的配置，还需要通过远程 Telnet 程序进行远程访问配置，或者通过 Web 的方式实现

路由器的远程配置。现在一般的路由器都有多种远程配置管理方式。

（2）路由器所支持的路由协议

因为路由器所连接的网络可能存在不同类型的网络，这些网络所支持的网络通信、路由协议有可能不一样，这时对于在网络之间起到连接桥梁作用的路由器来说，如果不支持一方的协议，那就无法实现它在网络之间的路由功能，为此在选购路由器时要注意所选路由器所能支持的网络路由协议有哪些，特别是广域网中的路由器。因为广域网路由协议非常多，网络也是相当复杂，如目前电信局提供的广域网线路主要有 X.25、帧中继、DDN 等多种。

（3）路由器的安全性保障

现在网络安全越来越受到用户的高度重视，无论是个人还是单位用户，而路由器作为个人、事业单位内部网和外部进行连接的设备，能否提供高要求的安全保障就极其重要了。目前许多厂家的路由器可以设置访问权限列表，控制哪些数据才可以进出路由器，实现防火墙的功能，防止非法用户的入侵。另外，路由器的 NAT（网络地址转换）功能，可以屏蔽内部局域网的网络地址，利用地址转换功能统一转换成外网地址，这样外部用户就无法了解到内部网的网络地址，进一步防止了非法用户入侵。

（4）丢包率

路由器作为数据转发的网络设备存在丢包率的现象。丢包率就是在一定的数据流量下，路由器不能正确进行数据转发的数据包在总的数据包中所占的比例。丢包率的大小会影响路由器线路的实际工作速度，严重时甚至会使线路中断。

（5）背板能力

背板能力通常是指路由器背板容量或总线带宽能力，这个性能对于保证整个网络之间的连接速度是非常重要的。如果所连接的两个网络速率都较快，而由于路由器的带宽限制，这将直接影响整个网络的通信速度。所以一般来说如果连接两个较大的网络，网络流量较大时应格外注意路由器的背板容量。

（6）吞吐量

路由器的吞吐量是指路由器对数据包的转发能力，如较高档的路由器可以对较大的数据包进行正确快速转发；而较低档的路由器则只能转发小的数据包，对于较大的数据包需要拆分成许多小的数据包来分开转发，这种路由器的数据包转发能力就差。吞吐量与背板容量有关。

（7）转发时延

转发时延指需转发的数据包最后一比特进入路由器端口到该数据包第一比特出现在端口链路上的时间间隔，这与背板容量、吞吐量紧密相关。

（8）路由表容量

路由表容量是指路由器运行中可以容纳的路由数量。一般来说越是高档的路由器路由表容量越大，因为它可能要面对非常庞大的网络。这一参数与路由器自身所带的缓存大小有关，一般的路由器也不需要太注重这一参数，因为一般来说都能满足网络需求。

（9）可靠性

可靠性是指路由器的可用性、无故障工作时间和故障恢复时间等指标，一般选购信誉较好、技术先进的品牌作保障。

4.5.2　路由器的连接

1．路由器与内网的连接

对内部局域网设备通过交换机或集线器连接，常用端口有 RJ45 和 SC。

（1）RJ45-to-RJ45

这种连接方式就是路由器所连接的两端都是 RJ45 接口的。需要注意的是，与集线器设备之间的连接不同，路由器和集线设备之间的连接不使用交叉线，而是使用直通线，也就是说，跳线两端的线序完全相同。

（2）SC-to-RJ45

这种情况一般是路由器与交换机光纤端口之间的连接，须借助 SC-to-RJ45 收发器才可实现两者之间的连接。收发器与交换机设备之间的双绞线跳线同样必须使用直通线。

2．路由器与外网的连接

路由器的主要应用是与外网连接。广域网通过路由器连接的物理线路多样，如电话线、同轴电缆、双绞线、微波或光纤等，对应的数据链路协议和物理层协议也多样。

（1）通过异步串口连接

这种异步串口在前面已有介绍，它主要是用来与 MODEM 连接，用于实现远程计算机通过公用电话网拨入广域网络。除此之外，也可用于连接其他终端。

（2）通过同步串口连接

路由器支持的同步串行端口类型比较多，如 EIA/TIA-232 接口、EIA/TIA-449 接口、V.35 接口、X.21 串行电缆和 EIA-530 接口。这些接口由专用终端、接口转换器或数字复用器等设备提供。

4.5.3　路由器的配置

1．路由器设置方式

可以用以下几种方式来设置路由器。

（1）超级终端方式。该方式主要用于路由器的初始配置，路由器不需要 IP 地址。基本方法是：计算机通过 COM1/COM2 口和路由器的 Console 口连接，在计算机上启用“超级终端”程序，设置“波特率为 9600，数据位为 8，停止位为 1，奇偶校验为无，校验为无即可。路由器的第一次设置必须通过这种方式进行。

（2）Telnet 方式。该方式配置要求路由器必须配置了 IP 地址。基本方法是：计算机通过网卡和路由器的以太网接口相连，用 Telnet 命令登录路由器配置界面。值得注意的是计算机的网卡和路由器的以太网接口的 IP 地址必须在同一网段。

（3）其他方式：AUX 口接 MODEM，通过电话线与远方运行终端仿真软件的计算机相连；通过 Ethernet 连接 TFTP 服务器或 SNMP 网络管理工作站。

2．路由器的工作模式

在命令行状态下，主要有以下几种工作模式。

（1）一般用户模式。主要用于查看路由器的基本信息，只能执行少数命令，不能对路由器进行配置。提示符为：Router>。

（2）使能（特权）模式。主要用于查看、测试、检查路由器或网络，不能对接口、路由协议进行配置。提示符为 Router#，进入使能模式命令为 Router>enable。

（3）全局配置模式。主要用于配置路由器的全局性参数。提示符为 Router（confg）#，进入全局配置模式命令为 Router#config ter。

（4）全局模式下的子模式。包括接口、路由协议、线路等。其进入和提示符如下。

接口模式：进入命令 Router（confg）#ineterface e0，提示符 Router（confg-if）#；

路由协议模式：进入命令 Router（confg）#rip，提示符 Router（confg-router）#；

线路模式：进入命令 Router（confg）#line con 0，提示符 Router（confg-line）#。

（5）监控模式。该模式主要用于 IOS 升级及恢复口令，不能用于正常配置。提示符为>，进入方法：在路由器加电 60 秒内，在超级终端连接状态下，同时按 Ctrl+Break 键。

3．路由器的内存体系

路由器内存一般有 ROM、FLASH、DRAM 和 NVRAM 等 4 种。ROM 相当于 PC 的 BIOS，路由器运行时首先运行 ROM 中的程序，该程序主要进行加电自检，对路由器的硬件进行检测。Flash 存放的是“IOS”，可以通过写入新版本对路由器进行软件升级。动态内存 DRAM 中的内容在系统掉电时会完全丢失，DRAM 中主要包含路由表、ARP 缓存、fast-switch 缓存、数据包缓存等。DRAM 中也包含正在执行的路由器配置文件“running-config”。NVRAM 中包含路由器配置文件“startup-config”，NVRAM 中的内容在系统掉电时不会丢失。

路由器启动时，首先运行 ROM 中的程序，进行系统自检及引导，然后运行 Flash 中的 IOS，并在 NVRAM 中寻找路由器的配置，并将装入 DRAM 中。ROM、NVRAM 容量大小不能调整；Flash、DRAM 容量大小能调整。

4．路由器配置内容

（1）基本配置

路由器的基本配置一般包括如下内容：路由器命名、配置口令及加密、配置相关接口、配置保存与加载、静态路由、默认路由等。基本配置是用户在使用路由器时必须进行的配置，是后续其他配置的基础。各型路由器的常用命令请参考路由器相关使用手册。

路由器也称作主机名（hostname），它会在系统提示符中显示，在集中配置一个多路由器环境的网络中，路由器的统一命名会给管理与配置路由器带来较大的方便。路由器的系统默认名字是 Router。命名需要在全局配置模式下完成。

路由器的口令主要有 enable 口令、console 口口令、aux 口口令及 Telnet 口令等，通过口令配置，增加系统的安全性。如果要使用 Telnet 登录网络中的路由器进行管理与配置，必须配置 Telnet 口令。

以太网接口的基本配置主要包括 IP 地址、速率、双工模式等。对于串口的基本配置，主要包括 IP 地址、封装协议、速率等。可以通过配置关闭或开启接口。

静态路由是手动配置的，当网络拓扑结构发生改变而需要更新路由时，网络管理员就必须手动更新静态路由信息。当某个网络只能通过一条路由出去时，使用静态路由即可。网络配置静态路由时就避免了动态路由更新所带来的系统和带宽开销。

默认路由也是由用户手动配置的，它作为到达目的网络的路由未知时所选择的路径。也就是当路由表中没有明确列出到达某一目的网络的下一跳时，将选择默认路由所指定的下一跳地址（默认路由的优先级最低）。实际上，路由器不可能知道到达所有网络的路由，因此，如想让内网用户能够访问互联网，必须都配置一条默认路由。

当前配置完成后，可以保存到启动配置 startup-config 中，也可以保存到 TFTP 计算机上。TFTP 服务器可以是一台装有并运行 TFTP 软件的计算机，可以从中导出和导入路由器的 IOS 软件和配置文件。

（2）路由协议配置

动态路由协议的两个基本功能为：①维护路由选择表，②以路由更新的形式将信息及时地发布给其他路由器。

基本路由算法可分为两种：距离矢量算法和链路状态算法。距离矢量算法确定网络中任意一条链路的矢量和距离，当从源端到目的端存在多条路径时，以距离最短 HOPS 为最优；链路状态（也称最短路径优先）算法需重建整个网络的拓扑结构，当从源端到目的端存在多条路径时，以代价最小为最优。

RIP 路由协议主要配置（宣告）RIP 协议的网段及其子网。在实验时为保证 RIP 路由的有效性，必须删除静态路由，可以保留默认路由。

OSPF 路由协议配置稍微复杂。图 4-23 为一个多区域的 OSPF 配置的网络结构。下面以图中的 R1、R2、R3、R4 为例说明多区域的 OSPF 配置的主要内容。OSPF 进程 ID 为 1-65535，只在路由器内部起作用，不同路由器一般要求不同。

图 4-23 中各路由器相关接口的 IP 地址如表 4-5 所示。

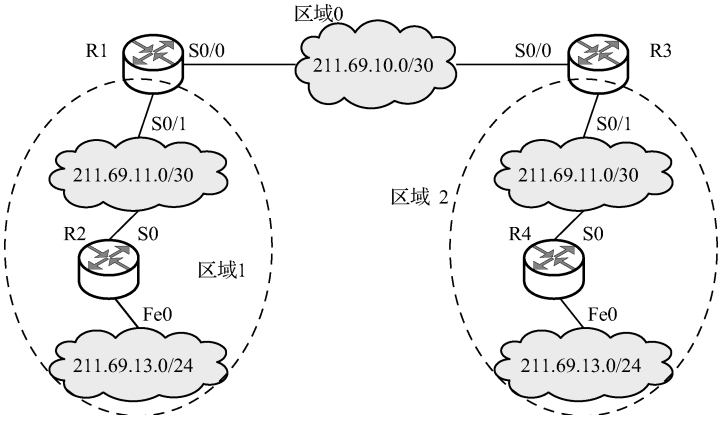


图 4-23　多区域的 OSPF 配置的网络结构

表 4-5　各路由器相关接口的 IP 地址

名　称	接口名称	IP 地址	子网掩码
R1	S0/0	211.69.10.1	255.255.255.252
	S0/1	211.69.11.1	255.255.255.252

续表

名　称	接口名称	IP 地 址	子网掩码
R2	S0	211.69.11.2	255.255.255.252
	Fe0	211.69.13.1	255.255.255.0
R3	S0/0	211.69.10.2	255.255.255.252
	S0/1	211.69.12.1	255.255.255.252
R4	S0	211.69.12.2	255.255.255.252
	Fe0	211.69.14.1	255.255.255.0

R1 路由器的主要配置如下。

启用 OSPF 路由协议并定义 OSPF 进程 ID 号为 100：Router（config）#router ospf 100

宣告直连网段及所在区域为 0：

```
Router（config-router）#networ k211.69.10.0 0.0.0.3 area 0
```

宣告直连网段及所在区域为 1：

```
Router（config-router）#network 211.69.11.0 0.0.0.3 area 1
```

R2 路由器的主要配置如下。

启用 OSPF 路由协议并定义 OSPF 进程 ID 号为 200：Router（config）#router ospf 200

宣告直连网段及所在区域为 1：

```
Router（config-router）#network 211.69.11.0 0.0.0.3 area 1
```

宣告直连网段及所在区域为 1：

```
Router（config-router）#network 211.69.13.0 0.0.0.255 area 1
```

R3 路由器的主要配置如下。

启用 OSPF 路由协议并定义 OSPF 进程 ID 号为 300：Router（config）#router ospf 300

宣告直连网段及所在区域为 0：

```
Router（config-router）#network 211.69.10.0 0.0.0.3 area 0
```

宣告直连网段及所在区域为 2：

```
Router（config-router）#network 211.69.12.0 0.0.0.3 area 2
```

R4 路由器的主要配置如下。

启用 OSPF 路由协议并定义 OSPF 进程 ID 号为 400：Router（config）#router ospf 400

宣告直连网段及所在区域为 2：

```
Router（config-router）#network 211.69.12.0 0.0.0.3 area 2
```

宣告直连网段及所在区域为 2：

```
Router（config-router）#network 211.69.14.0 0.0.0.255 area 2
```

在实际工作中，用户会遇到使用多个 IP 路由协议的网络。为了使整个网络正常工作，必须在多个路由协议之间进行路由再分配，这样不同的路由协议间就可相互通告路由信息了。这种情况称为多路由协议配置（重新分配路由或称再分布路由）。

图 4-24 中，R1 的 S0 端口和 R2 的 S0 端口运行 OSPF，在 R1 的 E0 端口运行 RIP-2，R3 运行 RIP-2，R2 有指向 R4 的 192.168.2.0/24 网段的静态路由，R4 使用默认静态路由。需要在 R1 和 R3 之间重新分配 OSPF 和 RIP 路由，在 R2 上重新分配静态路由和直连路由。

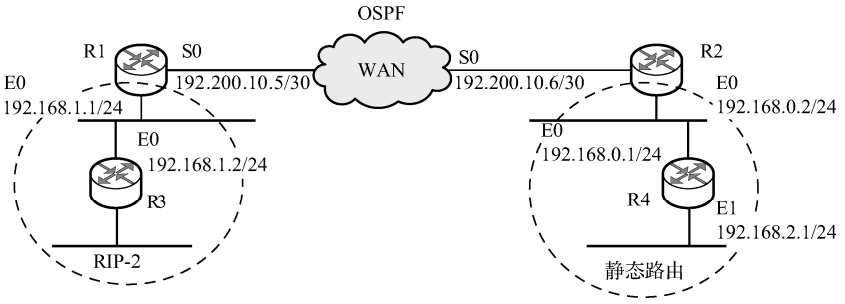


图 4-24　多路由协议配置的网络结构

R1 配置：

```
    Router（config）#interface ethernet 0
    Router（config-router）#ip address 192.168.1.1 255.255.255.0
    Router（config-router）#interface serial 0
    Router（config-router）#ip address 192.200.10.5 255.255.255.252
    Router（config-router）#router ospf 100
    Router（config-router）#redistribute rip metric 10（重新分配 RIP 路由，度量值为 10）
    Router（config-router）#network 192.200.10.4 0.0.0.3 area 0
    Router（config-router）#router rip
    Router（config-router）# version 2
    Router（config-router）#redistribute ospf 100 metric 1（重新分配 OSPF 路由，度量值为 1）
    Router（config-router）#network 192.168.1.0
```

R2 配置：

```
    Router（config-router）#interface loopback 1（R2 承担路由汇总，可减少网络中路由表的大小，loopback 1 为回送接口，是一个虚拟接口，为 OSPF 指定一个路由器 ID）
    Router（config-router）# ip address 192.168.3.2 255.255.255.0（该地址需是网络中唯一地址，保证此路由器 ID 在整个网络中是独一的）
    Router（config-router）#interface ethernet 0
    Router（config-router）# ip address 192.168.0.2 255.255.255.0
    Router（config-router）#interface serial 0
    Router（config-router）# ip address 192.200.10.6 255.255.255.252
    Router（config-router）#router ospf 200
    Router（config-router）# redistribute connected subnet
    Router（config-router）# redistribute static subnet
    Router（config-router）# network 192.200.10.4 0.0.0.3 area 0
    Router（config-router）#ip route 192.168.2.0 255.255.255.0 192.168.0.1
```

R3 配置：

```
    Router（config-router）#interface ethernet 0
    Router（config-router）# ip address 192.168.1.2 255.255.255.0
    Router（config-router）#router rip
    Router（config-router）# version 2
    Router（config-router）# network 192.168.1.0
```

R4 配置：

```
Router（config-router）#interface ethernet 0
Router（config-router）# ip address 192.168.0.1 255.255.255.0
Router（config-router）#interface ethernet 1
Router（config-router）# ip address 192.168.2.1 255.255.255.0
Router（config-router）#ip route 0.0.0.0 0.0.0.0 192.168.0.2
```

（3）广域网协议配置

路由器上比较常用的广域网协议配置包括 PPP 和 DDN 等。

① PPP 协议配置。

以图 4-24 所示网络中 R1 的配置为例进行说明。R1 的主要配置内容：

```
Router（config）#interface s0/0
Router（config-if）#ip address 211.69.10.1 255.255.255.252
Router（config-if）#enca ppp 系统封装 PPP 协议）
Router（config-if）#clockrate 130000（DCE 端需配速率，DTE 端不需配速率）
Router（config-if）#ppp authentication chap（默认为不验证，此步可省略）
Router（config-if）#no shutdown
```

注意，两端的验证密码须一致。

② DDN 专线连接的配置。

在实际工程中，路由器接 DDN 专线时，同步串口需通过 V.35 或 RS 232 DTE 线缆连接一个接口转换器，则路由器为 DTE，接口转换器为 DCE，由 DCE 端提供时钟。如果将两台路由器通过 V.35 线缆进行背对背直接相连，则必须由连接 DCE 线缆的一方路由器提供同步时钟。

以图 4-24 所示网络中 R1 背对背连接配置为例进行说明。R1 的主要配置内容：

```
Router1（config）#interface serial 0/0
Router1（config-if）#ip address 211.69.10.1 255.255.255.252
Router1（config-if）#clockrate 2000000（在 DCE 端配置同步时钟）
```

（4）远程访问配置

远程访问可以让网络延伸超越电缆网络的物理边界，延伸到世界的各个角落，只需要一个接收拨入连接的远程访问服务器、一个拥有拨号软件的远程访问客户及一对 MODEM 即可。

远程访问连接链路一般都是从网络服务提供商（ISP）那里租来的。远程客户和远程服务器必须共享至少一个网络传输协议，如 TCP/IP 协议。另外，需要一个链路协议，建立客户机和服务机之间的链路连接。用于建立连接的协议有 SLIP（Serial Line Internet Protocol）和 PPP（Point-to-Point Protocol），目前最常用的是 PPP 协议。

远程访问服务器是一个特殊类型的路由器，它们为通过拨号连接的远程用户提供网络访问服务。大多数访问服务器主要通过调制解调器拨入连接，拨入连接的总数目要由连接到访问服务器的所有租用线路中可用信道的数目来决定。

以图 4-24 所示网络为例来说明实现路由器拨号访问连接建立的主要配置。

R3 的主要配置：

```
Router（config）#interface group-async1（定义 group-async1）
Router（config-if）#ip unnumbered e0（引用 E0 端口的 IP 地址）
Router（config-if）#ip tcp header-compres passive（使用 IP 头指针压缩）
Router（config-if）#enca ppp（封装 PPP 协议）
```

```
Router（config-if）#async default routing（允许异步口路由）
Router（config-if）#async dynamic routing（允许异步口动态路由）
Router（config-if）#async mode interactive（异步口交互模式）
Router（config-if）#peer default ip address pool xlx（定义一名为 xlx 的地址池）
Router（config-if）#group-rang 1 8（将 MODEM 号 1～8 编组）
Router（config）#router rip
Router（config-router）#version 2（启用 RIPv2 协议）
Router（config-router）#network 211.69.15.0（宣告 211.69.15.0 网段）
Router（config-router）#exit
Router（config）#ip local pool xlx 211.69.15.1 211.69.15.8（定义 8 个 IP 地址）
Router（config）#line 1 8（定义 8 条 MODEM 拨号线路）
Router（config-line）#autoselect ppp（自动选择 PPP 协议）
Router（config-line）#login local（将读取用户名和密码）
Router（config-line）#modem inout（允许 MODEM 拨入拨出）
Router（config-line）#autocommand ppp（连接建立后，自动进入 PPP 模式）
Router（config-line）#transport input all（连接建立后，允许使用所有协议）
Router（config-line）#stopbits 1（定义 1 位停止位）
Router（config-line）#rxspeed 38400（设置接收速率）
Router（config-line）#txspeed 38400（设置发送速率）
Router（config-line）#flowcontrol hard（设置硬件流控）
Router（config-line）#exit
Router（config）#username user1 password 1（定义拨号用户名和口令，可成批定义）
```

使用小型程控电话交换机将异步口的 MODEM 和拨号连网计算机的 MODEM 连接起来，拨号的号码由异步口所连接程控交换机的端口号码决定。异步口的发送和接收速率必须和所用 MODEM 匹配。如果能够拨号，但连接总是建立不起来，可将异步口的速率设置得低一些。

习题

1．IP 地址的主要特点是什么？

2．简述 IP 地址的分类及其特点。

3．C 类网络使用子网掩码有无实际意义？为什么？

4．简述 IP 地址与路由的关系。

5．已知一个主机的 IP 和子网掩码分别为 130.50.15.6 和 255.255.252.0，求该 IP 在划分子网后，其子网号、主机号和网络地址。

6．某单位分配到网络号为 129.250.0.0，单位有 1000 台计算机，平均分布在 4 个不同的地点，选用子网掩码为 255.255.255.0，要求给每个地点分配一个子网号码，请给出分配的子网的网络地址、各个子网内主机号码的最大值和最小值。

7．两个单位分别拥有地址块 202.113.16.128/26 和 202.113.16.192/26，请给出聚合后的地址。

8．下面的前缀中，哪一个和地址 152.7.77.159 及 152.31.47.252 都匹配？请说明理由。

（1）152.40/13；（2）153.40/9；（3）152.64/12；（4）152.0/11。

9．简述路由器的功能。

10．IGP 和 EGP 这两类协议的主要区别是什么？

11．简述 RIP、OSPF 和 BGP 路由选择协议的主要特点。
12．简述 IP over SDH 的优点。
13．简述军事网络中建立 VPN 的好处。
14．简述三层交换机与一般路由器的差异。
15．路由器有哪些网络连接方式?

Chapter 5

第5章

军事网络服务

【主要内容】 介绍网络化信息服务核心思想、信息单元即插即用技术、服务器及 Web 技术，包括军事信息网络化服务的功能体系和实现流程，移动 IP 即插即用技术的工作原理，服务器的分类与选型，Web 服务的原理与技术等。

5.1 军事信息网络化服务概述

5.1.1 信息网络化服务体系

通过对全维、全域、全谱信息的网络化集成，军事网络为各级各类军事信息用户提供要素齐全的军事信息。军事信息服务的服务内容多样，信息服务的服务对象需求各异。信息用户既可以是传统的人员用户，也可以是连网的信息系统、指控系统和武器系统。网络环境下，信息服务不再是传统的针对特定用户提供的固定保障服务，而已形成网络化信息服务体系。

信息网络化服务体系就是指按既定的协议动态汇集、整合网络上的各类信息资源，将分散在不同地理位置、隶属于不同组织的信息系统，通过柔性重组、协同运作的方式实现系统资源共享、灵活配置和要素协同，形成一个高度共享、统一管理、合理分配、动态可调的信息服务池，为跨系统、跨平台、跨部门的各类信息用户提供便捷、完整、可靠、灵活的信息服务。这样，分类管理的信息用户可以在允许的范围内自主定制所需要的信息，服务体系自动将符合用户定制条件的信息分发给信息用户。

信息网络化服务体系采用面向服务的软件架构方法（SOA）进行构建。SOA 是一种不拘泥于具体实现技术的软件开发思想。SOA 最大的特点是强调中立接口和服务之间的松耦合，将网络中的资源抽象为服务，以实现资源的统一描述、管理、共享和整合，并支持应用的无缝集成、按需共享、动态组合。

网络化服务体系包括信息服务环境、计算存储环境和信息管理环境等实体，支持信息资源的生产管理、聚合提炼、共享服务和容灾备份。从系统功能实现的角度，主要需要目录服务、资源注册发现服务、信息分发调度服务、信息分发服务、资源监视服务和用户管理服务等。

1．资源注册发现服务

资源注册发现服务为网络上的服务资源（包括计算服务、信息服务）及数据资源提供发布界面和接口。资源发现服务为各类资源的用户（包括系统最终用户和系统开发者）提供查询相关资源的界面和接口，使用户能够快速、准确地搜索到想要的信息。在信息网络化服务体系中，信息分发调度服务、监视服务通过资源注册服务进行服务发布，并且能够通过资源发现服务被用户和开发者获取并访问。在网络的任意节点部署多个资源注册和发现服务，一方面分散每个服务节点的负载，同时多个节点之间保持数据同步，提高服务的抗毁性。

2．信息分发调度服务

信息分发调度服务是整个服务体系的业务核心，它将零散的信息服务单元组织在一起，统一管理和调度，形成信息分发服务池，提供更加可靠和连续的信息服务，实现资源的合理分配、动态调整。

3．信息分发服务

信息分发服务是最终向用户提供信息的服务节点。它不直接接收用户的定制请求，而是接收信息分发调度服务向其分配的服务请求，然后向用户系统输出信息。

4．信息定制服务

信息定制服务是整个信息网络化服务最终的用户交互界面。用户登录任意信息服务定制节点，都可以定制整个服务体系的信息。

5．资源监视服务

资源监视服务对服务资源的运行状态进行监视和管理，并提供界面和编程接口以对服务资源状态进行定制或查询。在信息网络化服务体系中，信息分发调度服务通过资源监视服务对信息分发服务进行状态监视，统一管理和调度。资源监视服务可同时监视多个服务资源。资源监视服务接收服务资源的状态报文，维护资源状态信息，并接收资源状态查询请求。

6．用户管理服务

用户管理服务实现用户统一认证和权限管理。在授权允许的范围内，所有服务节点都可为其服务。各个服务节点的用户数据保持同步。

军事信息网络化服务就是在通信网络的支撑下，通过服务的调度和组织，为军事信息用户提供即插即用的信息获取能力。通过调用信息服务提供的标准访问接口，用户能够在权限范围

内对网络中的各种信息进行查询、更新等访问操作，解决信息按需获取、存储和数据资源共享、数据容灾备份和负载均衡等问题。

5.1.2　信息网络化服务原理

在通信网络的支撑下，信息用户根据自己的需求获取信息服务，而不用关心信息服务处于何处。SOA 以“信息服务”的形式对系统功能进行封装和描述，具有开放性、跨平台、粗粒度、松耦合、可发现、可组合等特点，能够方便地实现现有系统之间、现有系统与新建系统之间的动态集成。

SOA 基于三种角色通过不同的操作来实现整个交互过程。信息服务提供者对自身所能提供的服务进行统一的描述，并把服务描述发布到服务注册中心。服务请求者通过查找操作从服务注册中心检索服务描述，然后使用服务描述与服务提供者进行绑定并调用服务实现或同它交互。

目前，Web Service 技术被公认为实现 SOA 架构的最好方式。在 SOA/Web Service 中，服务是一种部署于网络之上的可编程组件，它在异构的信息平台上构建了一个与平台无关、与语言无关的技术层，各种不同平台上的资源依靠这个技术层来实现彼此的集成。

SOA/Web Service 模型所构建的核心服务是实现基于信息服务获取信息的关键技术。核心服务通过建立分布式的服务集成框架和服务访问调用环境，为信息系统的集成提供信息服务开发和运行支撑平台，从而支撑业务功能通过标准化的服务方式对外发布、共享和访问，实现业务功能由本地调用向全网共享的方式转变。核心服务分别部署在服务调用者、服务提供者和支持中心，用来支撑面向服务的信息获取过程。

信息用户即服务调用者，主要部署服务会话管理、服务调用接口、服务状态通知等功能软件，实现服务异步调用、服务同步调用、服务通知、服务状态查询和订阅及用户调用会话管理、服务协议封装等。

各种信息源系统、信息处理系统即服务提供者，将信息发布到信息服务中心，提供信息定制界面以供用户对信息种类和要素进行选择，然后生成并分发用户所需信息。主要部署服务总线、服务容器及其中的各种业务服务，在该运行环境中支持运行资源注册服务、资源发现服务、资源目录服务、资源监视服务、用户管理和门户服务等通用服务，以及各专业的信息搜集、处理、分发等业务服务。业务服务通过服务总线集成、动态调度。

信息服务中心实现对信息用户的统一管理，接收用户的信息定制需求，查找定位服务位置、协议及状态，将服务请求传递给到合理的服务节点，按需分选、组织和分发信息产品。需要同时部署核心服务的服务调用者环境、服务提供者环境、服务总线和服务支撑工具，相互同步和备份各类核心数据、基础数据和全局共享数据。

网络化信息服务主要由信息服务中心和信息服务提供者基于策略自动实现，其流程如下。

1．接收用户申请

信息用户提出信息服务需求，信息服务中心的信息服务软件收到用户申请单，从用户申请单中提取信息服务的种类、格式和时间等要求。

2．组织信息产品

接收申请的信息服务中心根据元数据信息和当前数据服务节点负载状态，分配网上合适的

数据服务节点提供服务，单个或多个数据服务节点的信息组织软件按用户申请单确定的信息种类和格式进行信息的组织，生成满足用户要求的信息产品。

3．传递信息产品

信息发送软件根据用户系统目的端地址和主机标识为信息用户及时发送信息。

4．服务过程控制

信息服务中心实时在线分析每个信息用户的传输流量，当信道不能满足信息传输要求时，自动控制发送流量或选择其他路由。也可控制低速用户的信息申请容量，根据信道速率控制实时信息更新频率，确保信息服务的时效性。

5.1.3 信息网络化服务手段

信息网络化服务主要解决信息用户的自主按需使用问题，特别是军事信息系统动态配置中的信息服务问题。使得信息用户在整个网络体系中获取的信息是连续的，整个过程对信息用户是完全透明的。信息用户获取信息服务的手段主要有以下几种方式。

1．网络直接连接方式

使用统一分配的 IP 地址等互连参数，利用信息终端软件获取网络化服务。

2．拨号入网方式

通过加装拨号服务软件、信息定制软件或信息终端软件入网。

3．其他入网方式

可通过串口方式或数据链方式接收信息，或配备通用引接终端间接入网。

5.2 信息单元即插即用技术

在军事网络中，信息源、信息系统和信息用户等信息单元均要能通过有线或无线手段接入网络。但是，采用传统 IP 技术的信息单元在移动到另外一个子网时，由于不同的子网对应于不同的 IP 地址，不能使用原有 IP 地址进行通信，必须修改原 IP 地址为所在子网的 IP 地址。但是，若修改成新所在子网的 IP 地址，则原先网络中的信息单元又不能通过原有 IP 地址对其进行访问了。因此，实现信息单元的即插即用，必须保障信息单元能够本地或异地快速入网。

5.2.1 即插即用的概念

即插即用的概念源于计算机技术，原意是指不需要跳线和手动软件配置过程，当在支持即插即用的平台上插入一个即插即用设备时，可以在运行过程中动态地进行硬件自动检测和软件自动配置。所谓硬件自动检测就是在系统运行时，可以通过某种方式检测到设备存在或插入这

样的实际动作，从而得知有新的设备加入到硬件系统中；所谓软件自动配置就是在检测到设备后，自动为该硬件分配系统资源，加载设备驱动程序，然后告诉操作系统可以对设备进行操作及操作的途径和方法，同时告知设备都做了什么。即插即用的任务是把物理设备和软件相配合，在每个设备和它的驱动程序之间建立通信信道。

在军事网络中，信息单元即插即用是面向服务的网络化信息体系所展现的一个显著特征，指的是各类信息单元能够通过标准入网接口，随遇快速接入网络，能够被网络自动识别和自动配置，自动获得与身份相适应的软件功能，立即向网络共享信息或从网络获得信息服务，实现在需要的时间、需要的地点、与需要的用户进行端到端通信，从而适应信息单元的机动部署、信息网络的动态调整等需要。所谓的“即插”指的是能够快速接入网络，而“即用”则是能够迅速使用网络。速度快、可接入、能使用是即插即用的三个根本体现。

5.2.2　即插即用的实现

网络服务层主要由信息传送控制服务和通信网络资源管理服务等部分组成。信息传送控制服务实现应用和网络的“相互感知”，一方面对上层应用提供网络资源和网络能力发现，使应用能感知网络；另一方面了解应用的端到端信息传送需求，使网络能感知应用的传送需求，从而提供按需传送控制。

1．基于移动 IP 的实现方式

移动 IP 技术是实现即插即用的一种有效方式。采用移动 IP 技术，机动信息单元在跨网络、跨区域随意机动中，使用基于 TCP/IP 协议的网络时，不用修改计算机原来的 IP 地址，同时，继续享有原网络中的一切资源。简单地说，移动 IP 可在既定的网络中全方位地移动或漫游。

移动 IP 的技术特点是不需要对终端系统的 IP 地址进行改动，而使一个原本就有成熟网络拓扑的系统实现整体移动。对于在系统内部工作的设备，其移动是透明的，也就是感觉不到移动的存在，其使用网络方式、与外界的联系方式都不发生改变。另外，如果原系统中有部分没有跟随着移动，已经移动的系统与未做移动的系统之间的通信方式，与未发生移动前是完全一样的。

移动 IP 系统使用家网代理服务器与外网代理服务器的有效配合，可以在不改变系统原有配置的基础上实现对移动系统的定位，并且使用安全的隧道技术实时地实现移动系统与主系统的数据传输。使得只要在移动子系统接入的网络中，代理服务器就可以将其位置通知主系统，并且确保主系统不用做任何修改，就可以随时以主动或被动的方式同移动子系统进行数据交换。

在移动 IP 系统中定义了三种功能实体，如图 5-1 所示。

移动节点：一个主机或路由器，它从一个网络或子网移动到其他网络或子网，它改变位置时无须改变其 IP 设置，仍然可以通过其固定的 IP 地址进行通信。

家代理：一个连接到移动节点本地网络的主机或路由器，它保持移动节点的位置信息，当移动节点离开家乡网络时能够将发往移动节点的数据包传给移动节点。

外地代理：移动节点当前所在的外地网络上的一个主机或路由器，它能把由家代理送来的数据包转发给移动节点。

在图 5-1 中，三个子网分别是不同的 IP 子网，MT1 是归属于子网 l 的移动终端，HA1 与 FA1、HA2 与 FA2 分别是子网 1 与子网 2 的家代理与外代理。通常称子网 l 是 MT1 的家网，

称子网 2 是 MT1 的访问网或外网，MT1 由子网 1 漫游到子网 2 时，对 MT1 的漫游管理将由 FA2 与 HA1 及两个子网内的路由器协作完成。

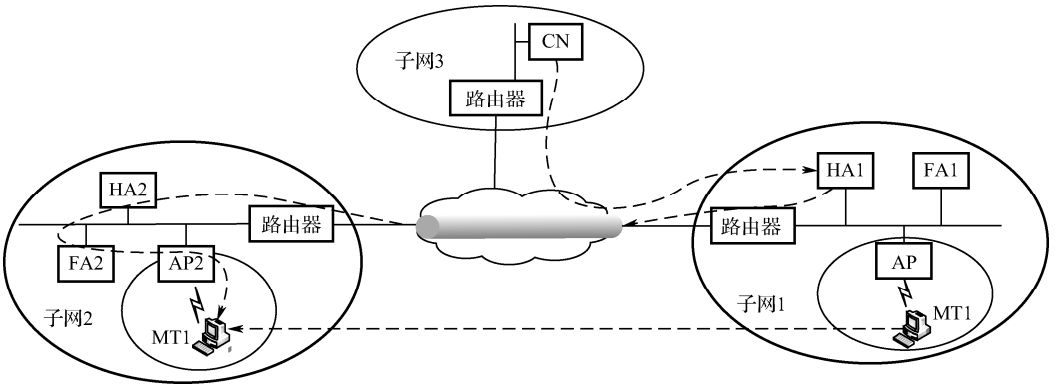


图 5-1　移动 IP 的三种功能实体

漫游协议的工作过程如下：

（1）MT1 利用代理搜寻功能检测自己已处于漫游状态，并获得转交地址；

（2）MT1 向 HA1 进行登录认证；

（3）HA1 将发给 MT1 的 IP 数据包利用其隧道发给 MT1；

（4）无论 MT1 是否漫游，它都使用 IPv4 协议发送 IP 包。

若由 CN 向 MT1 发送 IP 数据包，则数据包仍然寻找 MT1 原来的 IP 地址，故发出的数据包将首先到达子网 l，HA1 把这些 IP 数据包接收下来后，利用 HA1 至 FA2 的隧道把它们转送给 FA2，并由 FA2 把这些包转交给 MT1，图 5-1 中的虚线画出了 IP 包的路径。

当移动终端位于其家网中时，它可在没有移动服务支持下正常工作，也就是它可以像其他（固定）主机一样工作。当移动终端在外地代理登录时，家代理必须能在移动终端的家网地址中截获发往移动终端的数据包，这用到了代理 ARP 和强制 ARP，并通过隧道向移动终端目前登录的转交地址（通常是外地代理的 IP 地址）转发数据包。

2．移动 IP 中的 ARP 协议用法

所谓 ARP（Address Resolution Protocol）是指地址解析协议，它将目标节点的 IP 地址解析成节点的链路层地址，ARP 中定义了发送者和目标，由发送者发出询问，查找目标的数据链路层地址。工作过程如下：

（1）发送者向一条链路广播 ARP 请求消息，这条消息的目标 IP 地址域给出了想要寻找的 IP 地址对应的数据链路层地址；

（2）每个收到 ARP 请求消息的节点都将其中的目标 IP 地址与自己的 IP 地址相比较，如果相同就向该节点发送 ARP 应答，并在应答消息中注明自己的数据链路层地址。

在移动 IP 协议中为了进行正常的路由使用了两种 ARP 协议的特殊用法：代理 ARP 和强制 ARP。

代理 ARP 是指由一个节点代替另一个节点发送 ARP 应答，被代替的节点不可能或不愿回答对它的 ARP 请求，代理 ARP 节点将 ARP 请求的发送方和接收方的 IP 地址对换，填入 ARP 应答报文的发送和接收地址域中，在 ARP 应答报文的发送方硬件地址域填上配置好的链路层

地址（一般是它自己的硬件地址），接收应答的节点将这个链路层地址和需解析的节点的 IP 地址绑定。以后发往此 IP 目的地址的数据包的链路层地址将置为与它绑定的链路层地址。

强制 ARP 是一种 ARP 分组，目的是引起其他节点自动地更新它们的 ARP 缓存表项。强制 ARP 既可以使用 ARP 请求分组也可以使用 ARP 应答分组。无论是使用 ARP 请求分组还是 ARP 应答分组，ARP 发送方的协议地址和 ARP 接收方的协议地址都设置成 ARP 缓存中应更新的项的 IP 地址，并且 ARP 发送方的硬件地址置成缓存中 ARP 项应更新成的链路层地址。当使用 ARP 应答分组时，接收方的硬件地址也应设置成缓存中 ARP 项应更新成的链路层地址（在 ARP 请求分组中不使用这个域）。

ARP 分组必须作为本地广播分组来传输。当任何节点接收到任何 ARP 分组（请求或应答）并且这个节点的 ARP 缓存中已有此 IP 地址的解析项时，它都必须根据 ARP 分组中的 IP 地址和物理地址更新它的 ARP 缓存。这一规则也适用于与任何节点发出的 ARP 请求都不相匹配的 ARP 应答分组的情况。

3．家网中的工作步骤

代理 ARP 和强制 ARP 对移动终端的成功登录至关重要，需按照正确的次序使用。

当移动终端处于家网时，按照如下顺序工作：

（1）由于移动终端接收到一个家代理的代理公告，由此它判断出自己正处于家网之中，于是须向家网发送登录请求进行登录；

（2）在传输登录请求之前，移动终端使 ARP 请求处理功能恢复正常；

（3）移动终端为自己使用强制 ARP；

（4）移动终端传输它的登录请求；

（5）当移动终端的家代理接受移动终端登录请求时，它停止使用代理 ARP 来应答对移动终端的 ARP 请求分组，然后代表移动终端发送强制 ARP。如果家代理拒绝登录请求，则家代理不进行任何 ARP 处理（强制或代理）。

4．外网中的工作步骤

当一个移动终端离开它的家网时，其工作步骤为：

（1）当移动终端近期内没有从家代理收到代理公告而又从外地代理处收到代理公告时，它会认为它已经离开家网，进入了一个外地网，需外地网中的外地代理上进行登录；

（2）在传输登录请求之前，移动终端禁止它对 ARP 请求的正常处理，只对外地代理的 ARP 请求给予应答；

（3）移动终端发送它的登录请求；

（4）移动终端的家代理收到并接受登录请求，它代表移动终端使用强制 ARP 并开始用代理 ARP 对解析移动终端的链路层地址的请求予以回答。如果家代理拒绝登录请求，那么家代理不进行任何 ARP 操作。

5.2.3　移动 IPv6 工作原理

IPv6 通过无状态自动配置技术来支持移动节点互连。即使移动节点正在改变位置，移动 IPv6 仍然会保持移动节点赖以通信的现有连接。这对移动设备的自动组网非常有用。无状态自

动配置是指：IPv6 通过邻居发现机制为主机自动配置接口地址和默认路由器信息，使得从互联网到最终用户之间的连接不经过用户干预就能够快速建立起来。也就是说，移动节点在不同子网间移动时，运行在该节点上的应用程序不需要进行修改或重新配置。

这使得 IPv6 主机在离开家网后，仍能使用它的家乡地址，从而很好地维持原有的通信及连接。这种实现机制对于 IP 层以上是透明的，通信双方的 IP 层以上各层感觉不到移动节点的移动和 IP 地址的变化。这种即插即用体制对作战单元跨区域行动和协同作战尤其方便有利，不需要重新配置路由就可以实现“永远在线”的无缝连接。

移动 IPv6 中，每个移动节点都有一个对应家网前缀的“家乡地址（Home address）”。移动节点离开家网时，在新的子网链路上使用 IPv6 网络的“地址自动配置”机制，从而得到对应新的子网前缀的 IPv6 地址。如果简单地更新移动主机的 IP 地址，那么发往其家乡地址的数据包将不能到达主机。从而导致 IP 以上各层的连接在改变位置之后不能继续保持。因此，必须使通信各方同时保持移动节点“家乡地址”和新获得的所谓“转交地址（Care-of address）”。移动 IPv6 协议使得通信双方节点及家网上的相关路由器能够同时缓存移动节点的家乡地址及转交地址，这两种地址的联合称为“绑定（Binding）”。

移动节点宣告家网上路由器的这种“绑定”，使之成为自己的“家代理（Home agents）”。它帮助移动节点仍能以“家乡地址”和其他节点通信。而且，在通信节点了解了这种“绑定”之后，它就能绕开家代理，直接以移动节点的转交地址进行通信。

1．建立“家代理”

当移动节点连接外地链路时，它会通过“地址自动配置”机制来获得一个或多个由该外地链路子网前缀对应的 IPv6 转交地址。发往该转交地址的 IP 包直接路由到外网的移动节点，移动节点一旦获得转交地址，立即向家网上一个具有“家代理”功能的路由器发送一个“绑定更新”消息，通知该路由器自己位置的改变及新得到的转交地址，要求该路由器成为自己的“家代理”。路由器为该移动节点的“家乡地址”和“转交地址”建立一个“绑定”缓存条目，然后向移动节点回复“绑定认可”消息，正式成为它的家代理。

此后，一旦有目的地址是移动节点家乡地址的 IP 包被路由到家网上，家代理路由器就截获这些包，用 IPv6 协议封装，经隧道发往移动节点的转交地址。

2．移动主机通信规程及“三角路由”问题的解决

如果通信双方的数据包必须经过家网中转，就产生了所谓的“三角路由”。首先，家代理服务器负担增加；其次，传输延时增大，对一些延迟敏感的业务如音频、视频造成极大的损害。IPv6 比 IPv4 解决得相对容易，移动节点在收到从“家代理”经隧道转发过来的 IP 包时，在包扩展头中加入“绑定更新”选项，并向通信节点发送绑定更新后，将发往“家乡地址”的数据包直接发往“转交地址”，由此避免“三角路由”问题的出现。

而且，通信节点发往移动节点“转交地址”的数据包里包含了有关“家乡地址”的信息，从而使得移动节点能够理解这些 IP 包是发往其家乡地址的。它会把这些包的目的地址字段填上自己的家乡地址，再往上层提交，从而使“转交地址”对上层协议是透明的，上层连接得以保持。

3．“绑定”的更新和删除

当移动主机再次移动到另一个新的子网时，会获得新的转交地址，此时将重新登记绑定更新信息，使家代理及所有通信节点能够跟踪到移动主机位置的变化。当移动主机回到原地子网时，发送的将是“家乡地址”与“转交地址”字段同为“家乡地址”值的“绑定更新”消息。家代理及通信节点得到这样的消息，应该从所有已知绑定的列表中将有关该移动主机的绑定全部删除，所有通信恢复正常。

上述所有“绑定”都有其生存时限以避免绑定列表的无限扩张。当家代理路由器或通信节点绑定列表中为某个移动主机建立的绑定条目过期时，它就应该向移动节点发送一个“绑定请求”消息，使之收到后重新发送新的“绑定更新”消息，更新绑定的生存时间。

4．移动 IPv6 的关键技术

（1）“地址自动配置”机制

为了实现网络设备的即插即用，IPv6 提供了两种机制来实现主机 IP 地址及其相关信息的自动配置。一种是从 IPv4 继承来的动态主机配置协议（DHCP），又称为全状态自动配置。IPv6 还主要采用了另一种无状态自动配置机制。主机一旦接入网络，就用自己具有唯一性的接口 ID（48bit MAC 地址或其他具有唯一性的号码）附加在 IPv6 链路本地地址前缀 1111111010 和足够多的零之后，产生一个链路本地单播地址。然后主机向链路中所有路由器组播一个“路由器请求”消息，路由器返回一个全局单播地址前缀及其他相关配置信息。主机用此全局地址前缀加上自己的接口 ID 形成全局 128bit 地址，就可以参与网络通信了。

在此项主机配置过程中，没有人的手动干预或专门的主机配置服务器，是主机与路由器自动完成的，此即为“无状态地址自动配置”机制。移动主机移到其他子网时，就是使用这种机制得到自己对应当前链路的“转交地址”的。

（2）移动检测

当移动节点离开家网到其他链路时，可以使用任何可用的机制来检测到自己位置的移动。例如，在无线环境下，信号的消失可能意味着离开了原服务区，从而认为已经离开家网。但这样的低层协议是随着网络链路层技术的变化而变化的。要在 IP 层检测到节点位置的移动，移动 IPv6 采用“邻居发现”技术，其中包括“路由器发现”和“邻居不可达检测”。

路由器定期在本地链路上发送“路由器宣告”广播消息，移动节点接收到这样的消息，就为该路由器维护一个“默认路由器”条目，并记录下相应的子网前缀。“路由器宣告”消息中包含有“宣告间隔”选项，这意味着如果移动节点在这么长的时间内没有收到该路由器发来的新的“路由器宣告”消息，它就可以确定至少丢失了一个宣告消息。因此移动节点可以实现自己的策略来决定何时认为该路由器不可达，即自己位置已改变，从而转向其他路由器。

（3）“家代理发现”机制

移动节点离开本地链路时，使用该机制，在其家网上发现一个或多个具有家代理功能的路由器。此外，如果节点在外期间原来的“家代理”失效或消失，这种机制也能发挥作用。

首先，移动节点要向“移动 IPv6 家代理”的任意发送地址（Anycast address）发送一个“ICMP 家代理发现请求”消息，使用移动节点的转交地址作为该 IP 包的源地址。有家代理功能的路由器（该路由器某个网络接口加入了该任意发送地址）收到该消息后，应该向移动节点转交地址发送“ICMP 家代理地址发现应答”消息，返回家代理一个全球唯一地址，以及本地链路上

所有其他家代理按优先级排序的地址列表。移动节点收到这些信息之后，即可选择其一，发送“绑定更新”消息，得到自己的“家代理”。

（4）“邻居发现”机制

当移动节点离开家网时，它的家代理使用 IPv6 的“邻居发现”机制来截获发往移动主机“家乡地址”的数据包。

家代理代表移动节点在家网上广播“邻居广播”消息，将自己的数据链路层地址与移动节点在本地的每一个 IPv6 地址相关联。也就是说，除了链路层地址选项填入家代理自己的链路层地址外，“邻居宣告”消息中所有字段的设置应该与移动节点在家网时自己设置此消息的过程相同。这样，收到此消息的任何本地节点或路由器修改自己的“邻居缓存”，将移动节点的家乡地址与家代理的链路层地址进行联系。此后本地节点发往移动节点家乡地址的数据包，以及由其他路由器发来的目的地址是移动节点家乡地址的数据包被“家代理”截获，封装后经隧道转发给在外的移动节点。

5．移动 IPv6 的优势

移动 IP 有 IPv4 和 IPv6 两个版本，但 IPv6 相比 IPv4 有诸多优势。

（1）移动 IP 需要一定量的 IP 地址作为移动节点的转交地址，对于捉襟见肘的 IPv4 来说相当困难。而 IPv6 在拥有庞大地址空间的同时，提供了更好的自动配置的支持，生成转交地址相当方便。

（2）移动 IPv6 解决了所谓的“三角路由”问题。在其工作过程中，在外网的移动节点会将“绑定更新”消息发往与之通信的节点，它们之间 IP 包的路由无须经过家代理，也减轻了 IPv4 中家代理转发所有数据包带来的负担。

（3）移动 IPv6 中没有像移动 IPv4 那样使用 ARP 协议来截获数据包，所以无须考虑与 ARP 相关的特定数据链路层的性质。这种设置提高了协议的可靠性，简化了实现过程。

（4）移动 IPv6 无须外网代理，有着更加方便、完善的安全机制。其安全性建立在 IPv6 协议的安全机制之上，使用网络层 IPSec 来满足更新绑定时的安全需求，省去了很多额外的工作。IPSec 通过对数据加密、认证、完整性检查来保证数据传输的可靠性、私有性及保密性。

5.3 信息服务设备与技术

5.3.1 服务器的分类与选型

服务器是信息系统的核心设备，它完成信息的收集、处理、存储、分发等任务，因此也被称为信息处理网络的灵魂。服务器和显控台、通信处理设备、路由器等通过网络交换机连接，构成客户端/服务器结构。通信处理设备和路由器的输入和输出信息必须经过服务器处理，各显控台要获取信息并对系统实施控制，也必须经过服务器，因此可以说是服务器在“组织”和“领导”这些设备。

1．服务器的分类

（1）按网络规模划分

按网络规模划分，服务器分为工作组级服务器、部门级服务器和企业级服务器。工作组级服务器用于联网计算机在几十台左右或对处理速度和系统可靠性要求不高的小型网络，其硬件配置相对较低，可靠性不是很高。部门级服务器用于联网计算机在百台左右、对处理速度和系统可靠性中等的中型网络，其硬件配置相对较高，其可靠性居于中等水平。企业级服务器用于联网计算机在数百台以上、对处理速度和数据安全要求最高的大型网络，硬件配置最高，系统可靠性要求最高。需要注意的是，这三种服务器之间的界限并不是绝对的，而是比较模糊的，如工作组级服务器和部门级服务器的区别就不太明显，有的干脆统称为“工作组/部门级”服务器。

（2）按架构划分

按照服务器的架构，可以分为 CISC 架构的服务器和 RISC 架构的服务器。CISC（Complex Instruction Set Computer）是指“复杂指令集”，它是指英特尔生产的 x86（Intel CPU 的一种命名规范）系列 CPU 及其兼容 CPU（其他厂商如 AMD、VIA 等生产的 CPU），它基于 PC 体系结构。RISC（Reduced Instruction Set Computer）是指“精简指令集”，它是在 CISC 指令系统基础上发展起来的。RISC 架构的服务器指采用非英特尔架构技术的服务器，如采用 Power PC、Alpha、PA-RISC、Sparc 等 RISC CPU 的服务器。RISC 型 CPU 与 Intel 和 AMD 的 CPU 在软件和硬件上都不兼容。RISC 架构服务器的性能和价格比 CISC 架构的服务器高得多，在大型、关键的应用领域中居重要地位。

（3）按用途划分

按照使用用途，服务器又可以分为通用型服务器和专用型（或称“功能型”）服务器。通用型服务器是没有为某种特殊服务专门设计的可以提供各种服务功能的服务器，当前大多数服务器是通用型服务器。专用型服务器是专门为某一种或某几种功能专门设计的服务器，在某些方面与通用型服务器有所不同。例如光盘镜像服务器是用来存放光盘镜像的，那么需要配备大容量、高速的硬盘及光盘镜像软件。

（4）按外观划分

按照服务器的外观可以分为机架式服务器、刀片式服务器及机柜式服务器，其外观如图 5-2 所示。机架式服务器的外形看来不像计算机，而像交换机，有 1U（1U=1.75 英寸=4.45cm）、2U、4U 等规格。图 5-2（a）为机架式服务器，机架式服务器安装在标准的 19 英寸机柜里面。所谓刀片式服务器是指在标准高度的机架式机箱内可热插拔插多个卡式的服务器单元，实现高可用性和高密度并可轻松替换，如图 5-2（b）所示。每一块“刀片”实际上就是一块系统主板。它们可以通过“板载”硬盘启动自己的操作系统，类似于一个个独立的服务器，但可使用系统软件将这些母板集合成一个服务器集群，共享资源，为相同的用户群服务。机柜式服务器则指将多个服务器放在一个机柜中，如图 5-2（c）所示。

2．服务器的选型

信息服务器主要用于信息处理、数据记录、信息服务等。一般选用多 CPU、大容量内存、高速硬盘的企业级服务器，以满足信息系统对服务器在可靠性、实时性和处理能力等方面的高要求。

（a）机架式服务器　　（b）刀片式服务器　　（c）机柜式服务器

图 5-2　按外观划分的服务器种类

3．服务器集群架构

服务器需要连续不间断地工作。所有重要的数据都保存在服务器上，主要信息服务都在服务器上运行，一旦服务器发生故障，整个信息处理网络将瘫痪，大量数据将会丢失，造成的损失是难以估计的。因此，一般信息服务中心系统都使用两台服务器，构成双机热备份系统。

所谓双机热备份系统即两台服务器在系统中扮演两个不同的角色，一台为主服务器，一台为备份服务器。系统开机后，两服务器同时工作，只是由主服务器输出数据，备份服务器不输出，备份服务器实时监测主服务器的工作。一旦主服务器故障，自动进行切换，备份服务器自动上升为主服务器，完成主服务器的任务。

信息服务系统通过集群控制构件，把信息接收、处理和服务任务分配到两台服务器分布式工作，以提高系统处理能力和时效性。利用异地双机协同构件自动检测系统状态，当一台服务器故障时，自动切换到正常的服务器工作，以保证信息接收、处理和服务无缝正常运行。主备服务器也可以人工任务调配或切换。

所谓集群，就是将多台服务器通过专用设备或高速网络进行互连，从而构成一个整体，共同完成一个大型复杂事物处理和高可靠性任务。对用户而言，完全透明，视同一台服务器。一般地，集群管理将应用分为三类。

（1）互斥类：该类应用在任意时刻只能在一台服务器上运行，当该应用发生错误后，自动转移到另一台服务器上运行，对客户而言完全透明。

（2）主备类：该类应用可同时在两台服务器上以主备方式运行，处理相同事务，但只有主应用的结果对外输出。当主应用发生错误时，备应用自动升为主应用。当错误应用再次运行时，需与主应用进行数据同步。

（3）并行类：该类应用可在两台服务器上同时运行，相互独立。

5.3.2　Web 服务原理与技术

军事信息服务的系统支撑软件环境主要是数据库和 Web 服务器。信息管理与对外服务一般采用 B/S 结构。Web 服务器主要提供信息用户管理、数据管理、信息浏览分发等服务，用户通过浏览器访问信息系统的页面内容。Web 服务器一般要安装 IIS 或 Tomcat 等服务程序。

1．WWW 的起源与发展

WWW（即“World Wide Web”、“3W”、“Web”或“万维网”）是一个资料空间，包含很多 Web 页面文件，而 Web 页面中又包含许多超链接，指向网络任一服务器之中的任何资源。

利用超链接，Web 页面可以与其他 Web 页面进行关联，也可以与其他多媒体文件进行关联。

WWW 通过超文本传输协议（Hypertext Transfer Protocol，HTTP）传送给使用者，使用者通过点击链接来获得资源。万维网常被当成因特网的同义词，其实万维网是靠因特网运行的一项服务。

万维网的发明者叫蒂姆·伯纳斯·李。1989 年，伯纳斯·李撰写了《关于信息化管理的建议》，1990 年 11 月 12 日他和罗伯特·卡里奥（Robert Cailliau）合作提出了一个更加正式的关于万维网的建议，那年圣诞假期他制作了第一个万维网浏览器（同时也是编辑器）和第一个网页服务器。万维网中至关重要的概念——超文本起源于 20 世纪 60 年代，但是蒂姆·伯纳斯·李将超文本技术嫁接到了因特网上，并发明了全球网络资源唯一认证方法：统一资源标识符。

2．WWW 的工作原理

超文本由一个叫作网页浏览器（Web browser）的程序显示。网页浏览器从网页服务器取回称为“文档”或“网页”的信息并显示。通常显示在计算机显示器上。人可以跟随网页上的超链接（Hyperlink）取回文件，甚至可以送出数据给服务器。顺着超链接走的行为又叫浏览网页。相关的数据通常排成一群网页，又叫网站。

WWW 采用 B/S（Browser/Server，即浏览器/服务器）模式，透过 HTTP 存取世界各地的超媒体文件。超媒体和超文本的区别是文档内容不同。超文本文档仅包含文本信息，而超媒体文档还包含其他方式表示的信息，如图形、图像、声音、动画，甚至活动视频图像。

WWW 服务系统中，信息资源以页面（也称网页或 Web 页面）的形式存储在服务器（通常称为 Web 站点）中，这些页面采用超文本方式对信息进行组织，通过链接将一页信息链接到另一页信息，这些相互链接的页面信息既可放置在同一主机上，也可放置在不同的主机上。

在 Web 应用模式中，浏览器的任务是接收用户命令、发送请求信息、解释服务器的响应。每一个 WWW 服务器都有一个服务器进程，它不断地监听 TCP 的端口 80，以便发现是否有客户发出连接建立请求。如果有用户请求，服务器接收并响应用户请求，制作 Web 页面数据发送给提出请求的客户机。

WWW 的一般工作流程如图 5-3 所示。

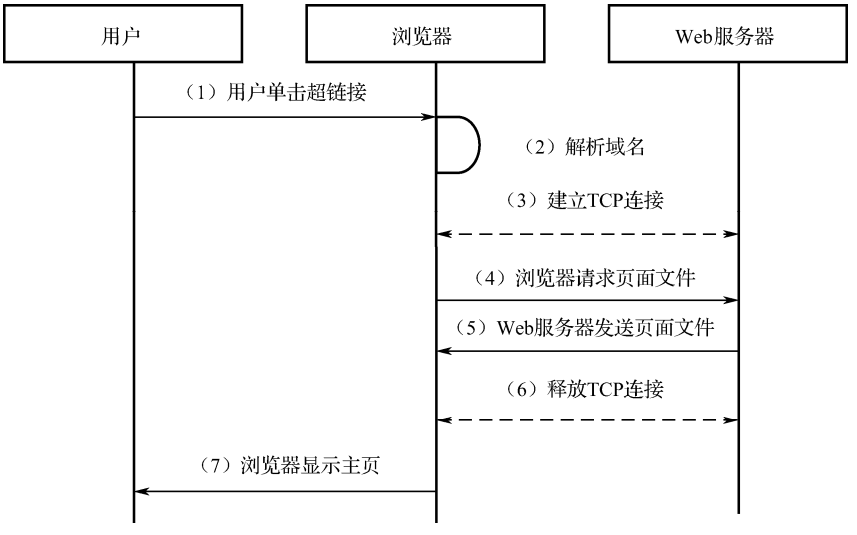


图 5-3　Web 服务技术流程

（1）用户使用浏览器以网页地址形式发出浏览请求；

（2）浏览器分析网页地址，向域名服务器请求解析网页地址中指定的主机域名的 IP 地址，得到 Web 服务器的 IP 地址；

（3）浏览器与相应 IP 地址的 Web 服务器建立 TCP 连接，端口号为 80；

（4）浏览器向 Web 服务器发出取网页地址中指定的页面文件命令；

（5）Web 服务器接收到请求后，给出响应，把网页地址中指定的页面文件发送给浏览器；

（6）释放 TCP 连接；

（7）浏览器接下来的工作是把接收到的页面文件内容显示给用户，构成用户所看到的“网页”。

WWW 服务的特点：以超文本方式组织网络多媒体信息；用户可以在世界范围内任意查找、检索、浏览及添加信息；提供生动直观、易于使用且统一的图形用户界面；服务器之间可以互相链接；可访问图像、声音、影像和文本信息。

3．WWW 的关键技术

URL、HTTP、HTML 构成了万维网的内核。统一资源标识符（Uniform Resource Locator，URL）是一个世界通用的负责对万维网上网页等资源进行定位的系统。超文本传送协议（HyperText Transfer Protocol，HTTP）负责规定浏览器和服务器怎样互相交流。超文本标记语言（HyperText Markup Language，HTML）的作用是定义超文本文档的结构和格式。

（1）怎样标识分布在整个因特网上的万维网文档？

WWW 使用统一资源定位符（URL）来标志万维网上的各种文档，包括指定各种网页的地址。它使网络上的每个文档都具有唯一的标识符。

URL 表示页面地址，用户可以利用 URL 指定要访问什么协议类型的服务器、互联网上的哪台服务器及服务器中的哪个文件，相当于文件名在网络范围的扩展。其应用如图 5-4 所示。

URL 的组成：协议、主机、路径及端口，如图 5-5 所示。

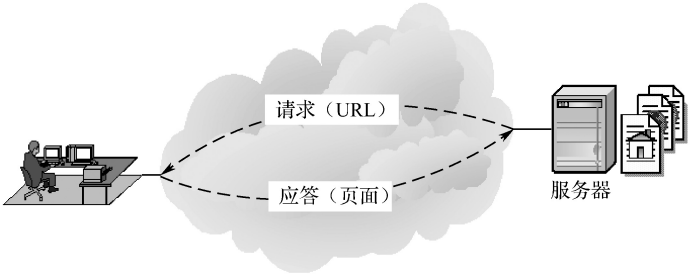


图 5-4　Web 应用模式

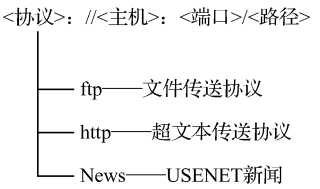


图 5-5　URL 的一般形式

<主机>是存放资源的服务器在因特网中的域名；<路径>指明（主机中某个）Web 页面文件，若省略则为默认的主页（通常为 index.htm 等）。

（2）如何实现万维网上的各种超链接？

在万维网客户程序与万维网服务器程序之间进行交互所使用的协议，是超文本传送协议 HTTP。HTTP 是一个基于 TCP/IP 的 Web 浏览器和 Web 服务器之间的应用层协议，它使用 TCP 连接进行可靠的传送，虽然 HTTP 本身是无连接的。

HTTP 的作用原理包括如下步骤。

① 连接：Web 浏览器与 Web 服务器建立连接，打开一个称为 socket（套接字）的虚拟文件，此文件的建立标志着连接建立成功。

② 请求：Web 浏览器通过 socket 向 Web 服务器提交请求。HTTP 的请求一般是 GET 或 POST 命令（POST 用于 FORM 参数的传递）。

③ 应答：Web 浏览器提交请求后，通过 HTTP 传送给 Web 服务器。Web 服务器接到请求后进行事务处理，处理结果又通过 HTTP 传回给 Web 浏览器，Web 浏览器再显示所请求的页面内容。

HTTP 精确定义了报文格式，保证通信不产生二义性。HTTP 有如下两类报文。

① 请求报文——从客户向服务器发送请求报文。HTTP 请求报文格式：一个请求行和若干个报头行，并可能在空行后带有报文体。请求行包括请求方法、被请求的文档及 HTTP 版本。

② 响应报文——从服务器到客户的回答。HTTP 应答报文格式：一个状态行和若干个报头行，并可能在空行后带有报文体。状态行包括 HTTP 版本、状态码、原因等。

（3）怎样使各种万维网文档都能在因特网上的各种计算机上显示出来，同时使用户清楚地知道在什么地方存在超链接？

WWW 采用超文本标记语言使得万维网页面的设计者可以很方便地用一个超链接从本页面的某处链接到因特网上的任何一个万维网页面，并且能够在自己的计算机屏幕上将这些页面显示出来。

Web 页面是利用 HTML 书写的结构化文档。它能够描述 Web 文档结构，创建超链接，定义格式化的文本、色彩、图像等。HTML 是 WWW 世界的共同语言，WWW 浏览器、编辑器和转换器等软件都需要按照统一的 HTML 标准处理页面。

HTML 是一个简单的标记语言。标记封装在“<”和“>”之中，标记不区分大小写字母，大部分标记成对出现，如<HEAD>和</HEAD>，部分标记（元素标记）单独出现，如<IMG>。HTML 把各种标签嵌入到万维网的页面中。这样就构成了所谓的 HTML 文档。HTML 文档是一种可以用任何文本编辑器创建的 ASCII 码文件。标记可附属性，如<IMG src = “http://netlab.nankai.edu.cn/lan.jpg” alt=“LAN Image”>

HTML 文档的基本结构标记示例代码如下，显示效果如图 5-6 所示。

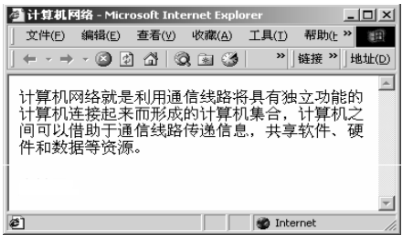


图 5-6　HTML 文档示例

```
<HTML>
<HEAD>
<TITLE>
计算机网络
</TITLE>
</HEAD>
<BODY>
计算机网络就是利用通信线路将具有独立功能的计算机连接起来而形成的计算机集合，计算机之间可以
```

```
借助于通信线路传递信息，共享软件、硬件和数据等资源。
    </BODY>
    </HTML>
```

习题

1．什么是信息网络化服务？
2．举例说明军事网络即插即用的含义？
3．简述移动 IPv6 实现信息单元即插即用的原理。
4．简述服务器的主要作用。
5．简述服务器集群的架构方法。
6．简述 WWW 的 3 大关键技术及其作用。
7．如何安装和配置一台 Web 服务器？

Chapter 6

第6章 军事网络管理

【主要内容】 介绍军事网络管理的基本概念、简单网络管理协议、网络故障及其排除方法，包括军事网络管理的需求、内容和方法，SNMP 网络管理的协议原理和系统组成，网络故障排除的一般方法和常用命令，网络故障排除典型步骤示例等。

6.1 军事网络管理概述

6.1.1 军事网络管理需求

军事网络管理是指对军事网络的运行状态进行监测和控制，使其能够有效、可靠、安全、经济地提供服务。通过监测了解当前网络状态是否正常、是否存在瓶颈问题和潜在危机。通过合理调节网络状态，提高性能，保证服务。

军事网络中传递的信息主要有数据、图像（视频）、语音 3 种类型，这 3 种信息一般在同一个网络信道中传输，必须确保对军事信息传输的响应时间。因此，需要对系统内部、系统之间使用的网络互连设备、网络信道、网络流量等进行监视、控制和管理，使网络中的各种资源得到有效利用，保证网络持续正常运行，当网络出现故障时能及时响应和排除故障。

军事网络管理实现对军事信息系统的用户管理，对有关设备状态、软件运行情况和计算机资源的监测，对双机系统的异地切换控制管理。记录所有用户资料、在线情况及设备监控数据、输入/输出信息，并提供事后分析工具；实现对信息系统的网络设备进行管理和远程配置，对网络运行状态进行监视、控制，对信息流量和带宽进行分配，对信息传输的优先级进行划分。

军事网络管理的目的是提升军事网络的运维信息感知、故障定位、故障处理能力，使得军事网络末端状态可监视、系统性能可度量、运行态势可显示、体系运维可控制。

（1）网络和设备管理

主要对路由设备、交换设备、网络服务器等网络运行状态进行监视、控制，实施网络运行参数配置、网络资源管理与调配、通信业务信息采集与分析、网络主要性能统计与分析等管理。

（2）网络业务管理

对数据、语音、多媒体等网络传输业务进行规划、开通、保障和服务，实施用户服务管理、业务指配管理、业务服务等级控制、业务质量监测、业务服务质量预警、业务资源管理、业务规划辅助决策等管理，并评估和处理网络与业务故障，发起故障处理流程。

（3）网络事务管理

面向网络与业务的运行组织、管理和值勤维护，实施网络与业务规划辅助决策、值交班管理、表报资料管理、业务处理流程管理、网络与业务故障处理、安全管理和系统管理等。

6.1.2 军事网络管理内容

军事网络管理包括对军事网络及其硬件、软件和人力的使用、综合与协调，以便对军事网络的各种资源进行监视、测试、配置、分析、评价及控制，主要包括以下内容。

1．配置管理

掌握和控制网络设备和网络服务的状态，提供设备及网络的各种配置情况和运行参数，并为其他网络管理功能提供信息。配置管理包括以下两大功能。

（1）拓扑图管理

拓扑图管理功能在系统初起将自动发现网络中各种类型的设备、设备内部的模块和端口及设备间的互连关系。拓扑图直观显示网络管理系统所要管理的全部对象，在拓扑图上可以方便地完成大部分网络管理工作。拓扑管理功能还可以及时反映网络拓扑的变化，添加或删除新的对象并更新显示。

（2）配置信息维护

建立网络管理对象数据库，对管理对象的重要运行参数进行集中管理和维护，如路由器的端口编号、端口类型、端口 IP 地址、端口连接的链路带宽、链路对端端口等信息的对照关系。

2．故障管理

检测、定位和排除网络硬件和软件中的故障。当出现故障时，该功能确认故障，常常要记录故障，找出故障位置并尽可能排除这些故障。故障管理包括以下两大功能。

（1）故障事件监测

网络管理员可对网络管理系统进行配置，对管理对象进行监测，并将故障事件转发给事件处理功能模块，故障监测对象主要以下几种：链路通断情况；路由器的端口状态；网络服务可用性；设备厂商定义的故障事件。

（2）故障事件处理

事件处理功能包括对事件进行过滤、相关性分析、传递、关联等处理，并将处理过的事件保存在事件日志中，最后分发给与此事件有关联的用户，用户需要在对发送上来的事件进行处

理后，确认该事件。

3．性能管理

测量网络中硬件、软件和媒体的性能。测量的项目有：整体吞吐量、利用率、错误率或响应时间等，目标是掌握网络资源的利用情况，并通过对各种性能参数的提取，反映网络的实际运行质量，为网络的优化运行及带宽的调整提供决策支持。性能管理包括以下两大功能。

（1）性能事件监测

性能事件监测通过主动轮询或接收网络上的各种事件来监视各种管理对象的性能。网络管理员应该能够通过对网络管理系统进行配置，对管理对象进行性能监测，定义性能门限，并将由于超越性能门限而触发的性能事件转发给事件处理功能。

（2）性能统计分析

性能统计分析通过对性能历史数据进行分析、统计和整理，计算性能指标，对性能状况做出判断，为网络规划提供参考。对数据进行检索和处理，生成性能趋势曲线，以直观的图形显示反映性能分析的结果。性能统计分析应实现以下功能：网络的各条链路的带宽利用率；各种业务对带宽的使用情况；流入、流出路由器的网络流量及细分。

4．服务质量管理

指定某种网络流量的优先级或网络带宽，或端到端延迟的实际质量级别。服务质量管理是网络管理系统的重要功能，可通过以下技术实现。

（1）定义排队方法

路由器使用的分组排队技术一般有先进先出（FIFO）、加权公平排队（WFQ）、定制排队（CQ）、优先级排队（PQ）四种。

（2）限制端口流量

即限制流入或流出某一网络设备接口的流量。根据 IP 优先级、进入的接口或 IP 访问表来限制某个网络设备端口的输入或输出。流量整形工具可平滑数据流的突发传输，从而防止网络阻塞和分组丢失。

5．安全管理

控制对网络资源的访问，以保证网络不被有意识或无意识地侵害，并保证重要信息不被未授权的用户访问。其主要内容是对网络资源和信息访问进行约束和控制，包括验证和控制网络用户的访问权限和优先级，同时还应检测和记录未经授权的用户对网络实施的非正常企图和操作。

6.1.3　军事网络管理方法

不同的管理对象具有不同的管理信息，不同级别的网络管理系统包含不同的管理信息。目前，军事网络管理已由“基于功能的管理”变为“基于结构的管理”，并向“基于质量的管理”发展，最终形成以用户为中心、面向不同业务的网络管理体系。

1．网络系统的管理

通过相应的网络管理系统软件实现对网络上的信息系统及其相关设备运行状态的监控和

切换，包括设备监控、计算机监控、应用软件监控、系统分级监控、系统性能管理、在线用户管理，并对集群、主备中心进行监视和切换控制。

（1）控制席位功能

控制各席位关机等。

（2）监控软件作业

监视席位应用进程，监视内容包括进程名、进程号、创建时间、CPU 运行时间等。控制受控进程的启动。

（3）监视业务席位

实时查看席位基本信息，包括操作系统、席位名称、IP 地址等。实时监视席位资源信息，包括内存、硬盘、CPU 利用率等。实时监视席位开机时间。

（4）实时监控服务器

实时查看服务器基本信息，包括操作系统、席位名称、IP 地址、开机时间等。实时监视服务器资源信息，包括内存、硬盘、CPU 利用率等。实时监视服务器应用进程，包括进程名、进程号、创建时间、CPU 运行时间等。控制服务器集群进程切换等。

（5）实时监控系统运行状态

实时监视系统运行模式，实时监控系统状态。

2．网络设备的管理

通过相应的网络管理系统软件对网络交换机、路由器等网络设备进行监控管理、流量控制、带宽分配和路由选择控制。

（1）监视网络设备

监视网络设备基本信息，包括设备描述、名称、IP 地址、运行时间、最大速率等。监视网络设备性能，包括利用率、流量、错误率等。监视网络设备端口状态，包括每个端口实时接通状态。

（2）控制网络设备

控制路由器等网络设备的端口使能。

（3）监视系统网络

路由跟踪，确定某一设备是由哪一台路由器接入的。检测网络节点的合法性，发现某一节点不是系统预期内的，予以告警。查找系统网络节点。

军事网络管理系统软件主要使用 TCP/IP 网络协议来构建管理信息传输网，实现各级各种管理信息的传输和交换。在管理协议与接口方面，各专业网的网络管理系统与被管设备的互连大多采用 SNMP 简单网络管理协议或厂家专用协议，而专业网的网络管理系统与综合网络管理系统的互连一般采用基于 CORBA 协议的分布式体系结构。即专业网的网络管理系统将 SNMP 和私有网络管理协议适配转换到第三方的 CORBA 协议上，由 CORBA 协议提供互通和统一的管理。下面仅对 SNMP 协议做简要介绍。

6.2 SNMP 网络管理协议

SNMP（Simple Network Management Protocol）称为简单网络管理协议，由一系列协议和

规范组成，提供一种从网络上的设备中收集网络管理信息的方法。虽然 SNMP 是 TCP/IP 协议族的一员，但它并不依赖于 IP。目前大部分 SNMP 都使用 IP 协议。

1．SNMP 的原理

基于 SNMP 的网络管理是目前技术成熟且被广为使用的网络管理体系结构。SNMP 管理体系结构由网络管理者、被管代理和管理信息库（MIB）三部分组成。SNMP 使用嵌入到网络设备中的代理来收集网络的通信信息和有关网络设备的统计数据。代理不断地收集统计数据，并把这些数据记录到 MIB 中。基于 SNMP 的网络管理体系结构如图 6-1 所示。

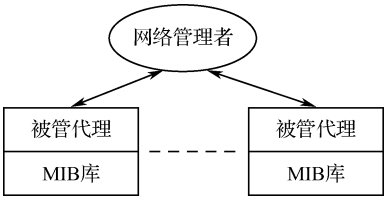


图 6-1　SNMP 协议体系结构

管理者（管理进程）实际上就是网络管理/网控中心，是管理指令的发出者。管理者通过各设备的管理代理对网络内的各种设备、设施和资源实施监视和控制。每个被管对象中都运行一个代理进程。代理负责管理指令的执行，并且以通知的形式向管理者报告被管对象发生的一些重要事件。

MIB 是被管对象结构化组织的一种抽象。它是一个包含统计信息及其他数据的数据库，由管理对象组成，各个代理管理 MIB 中属于本地的管理对象，各管理代理控制的管理对象共同构成全网的管理信息库。MIB 的每一项包含的信息有对象类型、语法、访问字段及状态字段等。对象类型为项的名称，通常为简单的名字。语法是一个值字段，通常为字符串或整型，并不是所有的 MIB 的项均包含值字段。访问字段用于定义项的访问权限，通常有以下四类：只读、可读/写、只可写或不可访问。状态字段包含指示值，标明 MIB 项是否为命令、可选或作废。

2．SNMP 的操作

基于 SNMP 的网络管理过程是一个异步的请求/响应过程。SNMP 实体不需要在发出请求后等待响应到来。SNMP 中包括四种基本的协议交互过程，即有四种操作：

（1）get 操作用来提取指定的网络管理信息；

（2）get-next 操作提供扫描 MIB 树和依次检索数据的方法；

（3）set 操作用来对管理信息进行控制；

（4）trap 操作用于通报重要事件的发生。

在这四个操作中，前三个是查询请求，由管理者发给代理，需要代理发出响应给管理者；最后一个则是自我报告，由代理发给管理者，但并不需要管理者响应。查询请求实际就是一种轮询的信息获取方法，而自我报告则是一种基于中断的信息获取方法。

网络管理者通过向代理的 MIB 发出查询信号得到信息，这个过程就叫轮询。轮询方法的缺点在于信息的实时性，尤其是错误的实时性。多久轮询一次、轮询时选择什么样的顺序都会对轮询的结果产生影响。轮询的间隔太小，会产生太多不必要的通信量；间隔太大，而且轮询时顺序不对，那么关于一些大的灾难性事件的通知又会太慢，这就违背了积极主动的网络管理目的。

与之相比，当有异常事件发生时，基于中断的方法可以立即通知网络管理者，实时性很强。但这种方法也有缺点。产生错误或自陷需要系统资源，如果自陷必须转发大量的信息，那么被管设备可能不得不消耗更多的事件和系统资源来产生自陷，这将会影响网络管理的主要功能。

3．基于 SNMP 的网络管理系统

网络管理系统监控软件由系统监控管理软件和系统监控代理软件两部分组成。系统监控管理软件安装于系统管理席，系统监控代理软件驻留于各计算机。整个监控系统基于 SNMP 实现。在每次开机后，被监控设备上的监控代理软件自动运行。

网络管理系统的组成如图 6-2 所示，图中硬件设备指的就是军事网络中的设备。显然，路由器、交换机等网络设备是支持 SNMP 标准的被管对象，本身具有代理软件；而通信管理器及一些席位计算机等则需开发转换代理软件，将不支持或没有 SNMP 协议的代理软件形成支持 SNMP 协议的代理软件。

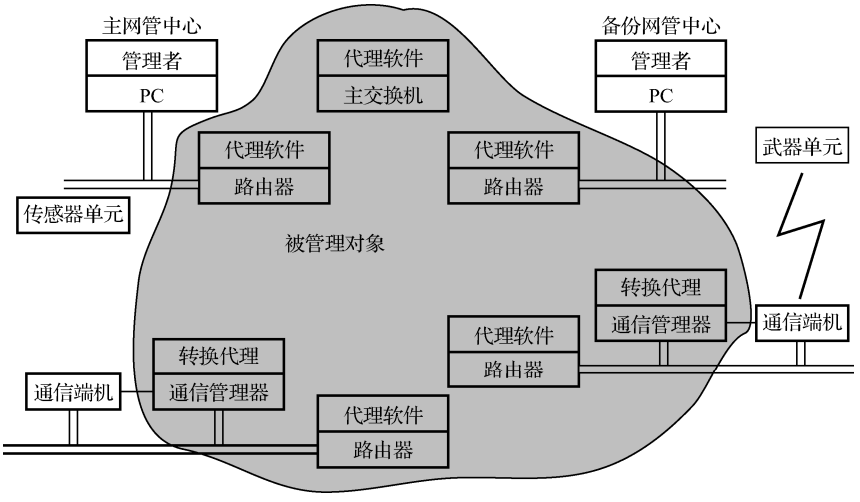


图 6-2　网络管理系统的组成

管理者和代理实际是两个遵循 SNMP 的软件，它们采用 C/S 模式，利用 SNMP 报文，通过 UDP 协议进行通信。客户进程在管理者上运行，服务器进程就是运行在被管网络设备上的代理软件。SNMP 利用 UDP 的两个端口（161 和 162）实现管理者和代理之间的管理信息交换。UDP 端口 161 用于数据收发，UDP 端口 162 用于代理报警（即发送 Trap 报文）。每一个支持 SNMP 的网络设备中都运行一个代理软件，此代理软件随时记录网络设备的各种情况，管理者通过 SNMP 查询或修改代理所记录的信息。

图 6-3 是使用 SNMP 的典型配置。整个系统必须有一个管理站，它实际上是网络管理中心。在管理站内运行管理进程。在每个被管对象中一定要有代理进程。管理进程和代理进程利用 SNMP 报文进行通信，而 SNMP 报文又使用 UDP 来传送。图中有两个主机和一个路由器。这些协议栈中带有阴影的部分是原来这些主机和路由器所具有的，而没有阴影的部分是为实现网络管理而增加的。

在网络管理系统运行过程中，代理进程及时发现故障，一方面以醒目的方式提醒值班人员做相应处理，同时控制系统自动做一些相应处理，以保证系统正常运行。可见，网络管理中心运行了管理进程，是网络管理系统的核心。由于网络管理需要消耗一定的带宽，因此，运行管理进程的网络管理中心应网络畅通，网络管理中心的管理人员也须有较强的网络管理知识和管理能力。

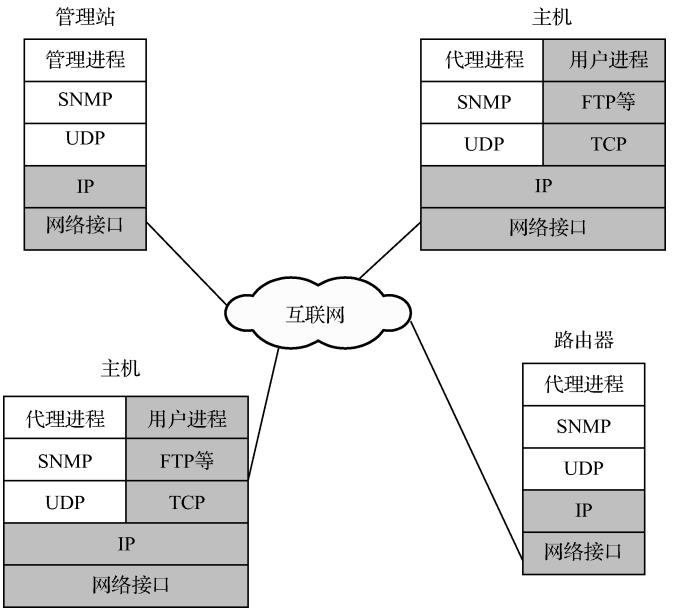


图 6-3　使用 SNMP 的典型配置

6.3 网络故障及其排除

军事网络的故障来源主要有两种：一是信息用户发现信息中断等不正常现象；二是系统值班人员采用网络管理系统软件、ping 等检查手段发现故障。这些故障的原因主要是设备故障、人为故障或非人力所能避免的灾害造成的故障。初步判断网络故障位置后，信息中断等局域网故障一般由网络管理中心的值班人员排查，路由器外端口网络中断等故障由网络专业人员排查。

6.3.1　网络故障排除一般方法

1．网络故障的常见原因

网络故障原因多种多样，总体上可分为硬件问题和软件问题，具体包括连通性故障、配置故障及协议故障。

（1）连通性故障

网络连通性是故障发生后应首先考虑的原因。连通性的问题通常涉及网卡、跳线、信息插座、网线、交换机、路由器等设备和通信介质。其中，任何一个设备的损坏都会导致网络连接的中断。连通性故障通常表现为以下几种情况：

① 计算机无法登录到服务器；

② 计算机无法通过局域网接入外部网络；

③ 在“网上邻居”中只能看到自己，而看不到其他计算机，从而无法使用其他计算机上的共享资源；

④ 计算机无法在网络内访问其他计算机上的资源；

⑤ 网络中的部分计算机运行速度异常缓慢。

以下原因可能导致连通性故障：

① 网卡未安装或未正确安装，或与其他设备有冲突；

② 网卡硬件故障；

③ 网络协议未安装或设置不正确；

④ 网线、跳线或信息插座故障；

⑤ 网络设备端口硬件故障。

（2）协议故障

没有网络协议，网络设备和计算机之间就无法通信，不能实现资源共享和上网。协议故障通常表现为以下几种情况：

① 计算机无法登录到服务器；

② 计算机在“网上邻居”中既看不到自己，也无法在网络中访问其他计算机；

③ 计算机在“网上邻居”中能看到自己和其他计算机，但无法访问其他计算机；

计算机无法通过局域网接入外部网络。

故障原因主要是：

① 协议未安装，包括 TCP/IP 及 PPP 等其他协议。

② 协议配置不正确，例如 TCP/IP 协议的基本参数有四个（包括 IP 地址、子网掩码、DNS、网关），任何一个设置错误都会导致故障发生。

（3）配置故障

配置错误也是导致故障发生的重要原因之一。服务器、计算机都有配置选项，如果对服务器、路由器等设备设置不当自然会导致网络故障。如果服务器权限设置不当，会导致资源无法共享的故障；如果计算机网卡配置不当，会导致无法连接的故障。网络用户对计算机设置的修改，也往往会导致一些令人意想不到的访问错误。配置故障通常表现为以下几种现象：

① 计算机只能与某些计算机而不是全部计算机进行通信；

② 计算机无法访问任何其他设备。

故障原因主要是：

① 服务器配置错误，如域控制器未设置或已到期的用户将无法登录服务器，服务器配置错误导致 Web、E-mail 或 FTP 服务停止，代理服务器访问列表设置不当将阻止有权用户接入外部网络；

② 网络设备配置错误，如路由器访问列表设置不当将会阻止有权用户接入外部网络。

2．故障排除的基本原则

（1）由近到远

从客户端开始检查。沿着客户端计算机→端口模块→水平线缆→跳线→交换机→路由器→广域网线路→对方机器这样一条路线，逐个检查，先排除自身端的可能故障。

（2）由外而内

如果某个设备存在故障，应该先从外部面板上的各种指示灯来辨别，然后根据故障指示检查内部的相应部件是否存在问题。例如交换机的 Power LED 指示灯为绿色表示电源供应正常，熄灭表示没有电源供应；Link LED 指示灯熄灭表示没有连接，闪烁表示端口被管理员手动关闭。

（3）由“软”到“硬”

发生故障后，不应动不动就先拿螺丝刀拆开设备，应先从系统配置或系统软件着手进行排查。排除了软件和配置上的各种可能原因，再可以怀疑是否出现硬件故障。

（4）先易后难

在故障分析时，必须先从简单操作或配置来着手分析。这样可以加快故障排除的速度，提高效率。当然，不管是什么样的故障，一定要在日常工作中积累经验，每排除一个故障都要用心地去回顾故障的根源及解决方法。这样才能不断地提高自己的能力，更好地保证网络的畅通。

3．故障排除的基本思路

（1）分层的故障排除思路

计算机网络故障通常有以下几种可能：物理层中物理设备相互连接失败或硬件及线路本身的问题；数据链路层网络设备的接口配置问题；网络层网络协议配置或操作错误；传输层的设备性能或通信拥塞问题。诊断网络故障时应该首先检查物理层，然后检查数据链路层，以此类推，设法确定通信失败的故障点，直到系统通信正常为止。

① 物理层：关注电缆、连接头、信号电平、编码、时钟和组帧，这些都是导致端口处于 down 状态的因素。故障主要表现在设备的物理连接方式是否恰当；连接电缆是否正确；MODEM、接口转换器等设备的配置及操作是否正确。确定路由器端口物理连接是否完好的最佳方法是使用“show interface”命令，检查每个端口的状态，解释屏幕输出信息，查看端口状态、协议建立状态。

② 数据链路层：关注封装协议和相关参数、链路利用率等。查找和排除数据链路层的故障，需要查看交换机、路由器的配置，检查连接端口共享同一数据链路层的封装情况。每对接口都要和与其通信的其他设备有相同的封装，可以使用“show”命令查看相应接口的封装情况。

③ 网络层：关注地址分配、路由协议参数等。地址错误和子网掩码错误是引起网络层故障最常见的原因；网络中的地址重复是网络故障的另一个可能原因；路由协议是网络层的一部分，在较复杂的网络中是排错重点关注的内容。排除网络层故障的基本方法是：沿着从源到目标的路径，查看路由器路由表，同时检查路由器接口的 IP 地址；如果路由没有在路由表中出现，应该通过检查来确定是否已经输入适当的静态路由、默认路由或动态路由；然后手工配置一些丢失的路由。

（2）分段的故障排除思路

将网络分为若干段，逐段测试，缩小故障范围，逐段定位网络故障并排除，流程图如图 6-4 所示。

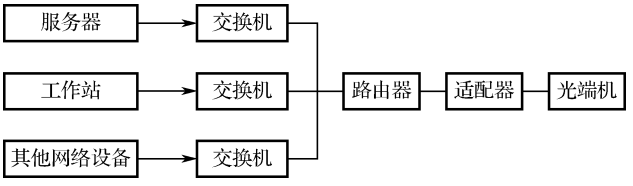


图 6-4　分段排除故障流程图

6.3.2 网络设备故障及其排除

计算机网络是一个复杂的综合系统，因此，网络故障诊断工作就显得困难繁杂。用户计算机的软/硬件问题及其与网络的连接问题一般较容易发现和排除，下面主要介绍交换机与路由器的故障诊断和排除方法。

1．交换机的故障类型及其排除方法

（1）交换机的硬件故障

交换机的硬件故障主要指交换机电源、背板、模块、端口等部件的故障。

① 电源故障。

由于外部供电不稳定，以及电源线路老化或雷击等原因导致电源损坏或风扇停转，从而导致电源不能正常工作。由于电源缘故而导致机内其他部件损坏的情况也经常发生。

如果前面板上的 Power 指示灯呈绿色，表示电源工作正常；如果该指示灯不亮，则说明交换机没有正常供电。这类问题很容易发现，也很容易解决，同时也是最容易预防的。

针对这类故障，首先应该做好外部电源的供应，一般通过引入独立的电力线来提供独立的电源，并利用带有稳压功能的 UPS 来避免瞬间高压或低压现象。如果条件允许，可以在机房内设置专业的避雷措施，避免雷电对交换机的伤害。

② 端口故障。

这是最常见的硬件故障，无论是光纤端口还是双绞线的 RJ45 端口，在插拔接头时一定要小心。如果不小心把光纤插头弄脏，将导致光纤端口污染而不能正常通信。很多人喜欢带电插拔接头，理论上是可以的，但是这样做将会增加端口的故障发生率。在搬运时不小心也可能导致端口物理损坏。如果购买的水晶头尺寸偏大，插入交换机时，也容易破坏端口。此外，如果接在端口上的双绞线有一段暴露在室外，这根电缆若被雷电击中，就会导致所连交换机端口被击坏，甚至造成更大的损失。

一般情况下，端口故障是某一个或某几个端口损坏。所以，在排除了端口所连计算机的故障后，可以通过更换所连端口来判断其是否损坏。遇到此类故障，可以在电源关闭后先用酒精棉球清洗端口，如果端口确实被损坏，那就只能更换端口了。

③ 模块故障。

交换机是由很多模块组成的，如堆叠模块、管理模块（也称为控制模块）、扩展模块等。虽然这些模块发生故障的概率很小，但是一旦出现故障，就会遭受巨大的经济损失。插拔模块方法不当，或者交换机在搬运机时受到碰撞，或者电源不稳定等，都可能导致此类故障的发生。

在排除此类故障时，首先确保交换机及模块的供电正常，然后检查各个模块是否插在正确的位置上，最后检查连接模块的线缆是否正常。在连接管理模块时，还要考虑它是否采用规定的连接速率、是否有奇偶校验、是否有数据流控制等因素。连接扩展模块时，需要检查通信模式是否匹配，如使用全双工模式还是半双工模式。

如果确认模块有故障，唯一的解决方法是立即更换。

④ 背板故障。

交换机的各个模块都是接插在背板上的。如果环境潮湿，电路板受潮短路，或者元器件因高温、雷击等因素而受损，都会造成电路板不能正常工作。在电源供电正常的情况下，如果交

换机的各个内部模块都不能正常工作，极有可能是背板坏了。

解决背板故障的唯一方法是更换背板。

⑤ 线缆故障。

这类故障从理论上讲不属于交换机本身的故障，但在实际使用中，电缆故障经常导致交换机系统或端口不能正常工作，所以也把这类故障归入交换机硬件故障。例如接头接插不紧，线缆制作时顺序排列错误或不规范；线缆连接时应该用交叉线却使用了直通线；光缆中的两根光纤交错连接，错误的线路连接导致网络环路等。

从上面几种硬件故障来看，机房环境不佳极易导致各种硬件故障。所以，在建设机房时，必须先做好防雷接地、供电电源、室内温度、室内湿度、防电磁干扰和防静电等环境的建设，为网络设备的正常工作提供良好的环境。

（2）交换机的软件故障

交换机的软件故障是指系统软件及其配置上的故障。

① 系统软件错误。

交换机系统是硬件和软件的结合体。在交换机内部有一个可刷新的只读存储器，其中保存着这台交换机正常工作所必需的软件系统。和 Windows、Linux 一样，由于软件设计的原因，这些软件中也存在着漏洞甚至错误。在某些情况下，这些漏洞或错误将会导致交换机满载、丢包、错包等情况的发生。所以交换机系统提供了诸如 Web、TFTP（普通文件传输协议）等方式来下载并更新系统软件。当然在升级系统时，也有可能发生错误。

对于此类故障，需要经常浏览设备厂商网站。如果有新的升级软件或补丁推出，应及时更新。

② 配置不当。

由于对交换机不熟悉，或者由于各种交换机配置不一样，或一时疏忽，在配置交换机时可能会出现错误的配置，从而导致交换机不能正常工作。例如 VLAN 划分不正确将导致网络不通、端口被错误地关闭、交换机和网卡的传输模式配置不匹配等。这类故障有时很难发现，需要有一定的经验。如果不能确定配置是否正确，可先恢复为出厂默认配置，然后一步一步地配置。在配置之前，应仔细阅读相关资料。每台交换机都有详细的安装手册、用户手册，甚至对每类模块都有详细的讲解。

③ 密码丢失。

一旦忘记密码，可以通过一定的操作步骤来恢复或重置系统密码。有的交换机操作比较简单，在交换机上按下一个按钮就可以了，而有的则需要通过一定的软件操作才能解决。此类情况一般在人为遗忘或交换机发生故障而导致数据丢失时才会发生。

④ 外部因素。

由于病毒或黑客攻击等情况的存在，有可能某台主机向所连接的端口发送大量不符合封装规则的数据包，造成交换机处理器过分繁忙，致使数据包来不及转发，进而导致缓冲区溢出，产生丢包现象。还有一种情况就是广播风暴，它不仅会占用大量的网络带宽，还将占用大量的 CPU 处理时间。网络如果长时间被大量广播数据包所占用，正常的通信就无法进行，网络速度也将变慢或导致网络瘫痪。

一块网卡或一个端口发生故障都有可能引发广播风暴。由于交换机只能分割冲突域，而不能分割广播域，所以当广播包的数量占到通信总量的 30%时，网络的传输效率就会明显下降。

总的来说，软件故障比硬件故障难查。解决故障时，可能不需要花费过多的金钱，却需要较多的时间。最好在平时的工作中养成记录日志的习惯。每当发生故障时，及时做好故障现象

记录、故障分析过程、故障解决方案、故障归类总结等工作，以积累和丰富排除故障的经验。例如有时在进行配置时，由于种种原因，当时没有对网络产生影响或没有发现问题，但也许几天以后问题就会逐渐显现出来。如果有日志记录，就可以联想到是否前几天的配置有错误。由于很多时候都会忽略这一点，以为是其他方面出现了问题，走了许多弯路之后，才找到问题所在。所以记录日志及维护信息是非常必要的。

2．路由器的故障类型及其排除方法

如果某系统内部能正常交换信息，但系统之间不能正常交换信息，则故障很可能出现在广域网的连接上。广域网设备主要包括路由器及各系统路由器之间的串行通信线路。路由器故障可以出现在硬件上也可以出现在软件上，大部分故障出现在软件上。

（1）路由器的硬件故障

路由器的硬件包括 RAM/DRAM、NVRAM、Flash、ROM、CPU、各种端口及主板和电源。硬件故障一般可以从 LED 指示灯上看出。例如，电源模块上有一个绿色的 PWR（或 Power）状态指示灯。当这个指示灯亮时，表示电源工作正常。接口模块上还包括 Online 和 Offline 指示灯及 TX、RX 指示灯，Rx 指示灯为绿色表示端口正在接收数据包；如果为橙色，则表示正在接收流控制的数据包。Tx 指示灯为绿色表示端口正在发送数据包；如果为橙色，则表示正在发送流控制的数据包。

硬件故障有时也可以从启动日志中查出或在配置过程中看出。常见的硬件故障是接口故障，下面介绍接口故障的排除方法。

① 串口故障排除。

串口出现连通性问题时，为了排除串口故障，一般从“show interface serial”命令开始，分析它的屏幕输出报告内容，找出问题所在。串口报告的开始提供了该接口状态和线路协议状态。接口和线路协议的可能组合有以下几种。

一是串口运行、线路协议运行。这是正常的工作状态。该串口和线路协议已经初始化，并且正在交换协议的存活信息。

二是串口运行、线路协议关闭。这个显示说明路由器与提供载波检测信号的设备连接，表明载波信号出现在本地和远程的调制解调器之间，但没有正确交换连接两端的协议存活信息。可能的故障是路由器配置问题、调制解调器操作问题、租用线路干扰或远程路由器故障、数字式调制解调器的时钟问题等，通过链路连接的两个串口不在同一子网上也会出现这个报告。

三是串口和线路协议都关闭。可能是电信部门的线路故障、电缆故障或调制解调器故障。

四是串口管理性关闭和线路协议关闭。这种情况是因为在接口配置中输入了“shutdown”命令。通过输入“no shutdown”命令，可以打开管理性关闭。

五是接口和线路协议都运行的状况下，虽然串口链路的基本通信建立起来了，但仍然可能由于信息包丢失和信息包错误而出现许多潜在的故障。正常通信时接口输入或输出信息包不应该丢失，或者丢失的量非常小，而且不会增加。如果信息包丢失规律性增加，表明通过该接口传输的通信量超过接口所能处理的通信量。解决的办法是增加线路容量。查找其他原因发生的信息包丢失，查看“show interface serial”命令的输出报告中输入/输出保持队列的状态。当发现保持队列中信息包数量达到信息的最大允许值时，可以增加保持队列设置的大小。

② 以太接口故障排除。

以太接口的典型故障问题是：带宽的过分利用；碰撞冲突次数频繁；使用不兼容的帧类型。

使用“show interface Ethernet”命令可以查看该接口的吞吐量、碰撞冲突、信息包丢失及和帧类型有关的内容等。

通过查看接口的吞吐量可以检测网络的带宽利用状况。如果网络广播信息包的比例很高，网络性能开始下降。光纤网转换到以太网段的信息包可能会淹没以太接口。互联网发生这种情况可以采用优化接口的措施，即在以太接口使用“no ip route-cache”命令，禁用快速转换，并且调整缓冲区和保持队列的设置。

两个接口试图同时传输信息包到以太网电缆上时，将发生碰撞。以太网要求冲突次数很少，不同的网络要求是不同的，一般情况下发现每秒有三五次冲突就应该查找冲突的原因了。碰撞冲突产生拥塞，碰撞冲突的原因通常是敷设的电缆过长、过分利用，或者“聋”节点。以太网络在物理设计和敷设电缆系统管理方面应有所考虑，超规范敷设电缆可能引起更多的冲突发生。

如果接口和线路协议报告运行状态，并且节点的物理连接完好，可是不能通信。引起该问题的原因也可能是两个节点使用了不兼容的帧类型。解决问题的办法是重新配置使用相同帧类型。如果要求使用不同帧类型的同一网络的两个设备互相通信，可以在路由器接口使用子接口，并为每个子接口指定不同的封装类型。

③ 异步通信口故障排除。

互连网络的运行中，异步通信口的任务是为用户提供可靠服务，但它又是故障多发部位。异步通信口故障一般的外部因素是：拨号链路性能低劣；电话网交换机的连接质量问题；调制解调器的设置。检查链路两端使用的调制解调器：连接到远程 PC 端口调制解调器的问题不太多，因为每次生成新的拨号时通常都初始化调制解调器，利用大多数通信程序都能在发出拨号命令之前发送适当的设置字符串；连接路由器端口的问题较多，这个调制解调器通常等待来自远程调制解调器的连接，连接之前，并不接收设置字符串。如果调制解调器丢失了它的设置，应采用某种方法来初始化远程调制解调器。简单的办法是使用可通过前面板配置的调制解调器；另一种方法是将调制解调器接到路由器的异步接口，建立反向 telnet，发送设置命令配置调制解调器。

“show interface async”命令和“show line”命令是诊断异步通信口故障使用最多的工具。“show interface async”命令输出报告中，接口状态报告关闭的唯一的情况是接口没有设置封装类型。线路协议状态显示与串口线路协议显示相同。“show line”命令显示接口接收和传输速度设置及 EIA 状态显示。可以认为“show line”命令是接口命令的扩展。查看“show line”命令输出的 EIA 信号可以判断网络状态。

确定异步通信口故障的一般步骤：检查电缆线路质量；检查调制解调器的参数设置；检查调制解调器的连接速度；检查 rxspeed 和 txspeed 是否与调制解调器的配置匹配；通过“show interface async”命令和“show line”命令查看端口的通信状况；从“show line”命令的报告检查 EIA 状态显示；检查接口封装；检查信息包丢失及缓冲区丢失情况。

（2）系统丢失

这里的系统是指 IOS（Internet Operating System），它就是路由器的一切配置运行的基础。它保存在 Flash 中，有时因操作失误或其他不可预料的原因（如突然断电），致使 Flash 中的 IOS 丢失，导致路由器无法正常启动。

出现此情况时，还可以使用保存在 ROM 中的备份操作系统软件，这个备份 IOS 通常比 Flash 中的 IOS 版本低一点，但足以让路由器启动和工作。为了让路由器正常工作，必须重新下载新

的 IOS 到 Flash 中。如果 Flash 的空间足够大，还可以保存多个 IOS 软件，并可以选择使用哪个版本的系统。为了能够在发生此类故障后迅速恢复，最好先把 IOS 软件保存在安全的服务器中。

（3）系统缺陷

像 Windows 系统经常受各种病毒的侵扰而死机一样，IOS 的系统缺陷也会致使路由器瘫痪。IOS 也有安全上的缺陷，如果不及时升级，路由器会成为他人的攻击目标。随着路由器的发展，现在有的路由器有自动防御攻击的功能，如抵御 DOS 攻击、防止密码猜测等。

IOS 的系统缺陷一般不通过补丁程序来修补，而是替换为全新的 IOS。一旦发现系统故障，路由器厂商会及时在网站上公布该故障、受影响的系统和相应的新的 IOS 软件，须选择适合的路由器型号的 IOS 版本进行替换。

（4）密码丢失

路由器中的密码有两个地方需要设置。访问路由器时有两个基本的访问模式：用户模式和管理模式。安全起见，在进入这两个模式时均需要设置密码。万一密码丢失，路由器提供了密码恢复方法。路由器除了这两个基本访问模式（用户模式和管理模式）外，还有一种 RXBOOT 模式，在这个模式下可以很方便地恢复路由器密码。当然只有计算机通过 CONSOLE 口建立超级终端连接后才能进入。还有些路由器在面板上提供了更方便的 RESET 键，只要复位几次即可恢复原始密码。

（5）配置文件丢失

这也是经常发生的故障。首先来看路由器的启动过程：路由器硬件加电自检，运行 ROM 中的硬件检测程序，检测各组件能否正常工作；然后运行 ROM 中的 BootStrap 引导程序，寻找并载入 IOS 系统文件；在 IOS 装载完毕后，系统首先在 NVRAM 中搜索 Startup-Config 文件，进行系统配置。

如果 NVRAM 中存在 Startup-Config 文件，则将该文件调入 RAM 中并逐条执行。随后依据配置文件中的命令进行接口地址设置、路由处理等工作。如果不能成功引导 Startup-Config 文件，系统则进入 Setup 模式，以人机对话方式进行路由器的初始配置。

也就是说如果启动配置文件丢失，系统不能对路由器进行具体配置，无法完成所需的功能。若要恢复配置文件，必须先连接到路由器上，通过 TFTP 方式将计算机上的备份配置复制到 NVRAM 上。所以每次修改过路由器的配置后都要做好备份工作。

（6）配置错误

常见的配置错误包括：路由协议配置错误、IP 地址和掩码错误、ACL（访问控制列表）错误、修改配置后没有保存等。例如，访问控制列表错误就是一个典型的配置错误。ACL 是一张应用于路由器某个接口的一组命令列表，这个列表告诉路由器哪种数据包应该接收、哪种必须禁止，从而达到数据过滤效果，这是一个有效控制网络安全的手段。这个列表的书写涉及源地址、目标地址、端口号几个参数。ACL 是顺序执行的，而且在所有 ACL 的最后会有一个默认的、不可见的“deny any”语句，即禁止任何通信。所以在定义某个 ACL 时，至少有一个 PERMIT 语句，否则这个访问列表是没有意义的。初学者往往会忽略这一点而导致网络不通，还有可能会写错 ACL 中使用的端口号，ACL 语句的顺序不恰当，或者通配符（WILDCARD，可能会和掩码混淆）不正确，接口应用错误（OUT 和 IN 混淆），等等。

（7）外部因素

这是指除路由器之外的因素导致疑似路由器故障。例如，客户端计算机的网卡故障、线缆接头不正确、线缆串扰等因素可能会引起数据碰撞、网络流量增大、路由器负载增加，导致网

络变慢甚至瘫痪。如果拨号路由器的 WAN 口线路发生故障，就会导致不能拨号。

路由器相比于交换机而言，具有强大的系统检测和日志记录功能。大部分故障都有详尽的描述，通过日志可以很方便地查找到故障原因。

首先，排查路由器之外的故障，并检查路由器的外部表象，可有效辨别硬件故障所在。例如，是否有客户端计算机故障，是否有外部线路上的故障，下联的交换机是否有故障，是否有接头上的故障，电源模块、端口模块等插槽的 LED 指示灯是否有故障指示，风扇是否旋转，端口的连接是否正确，等等。虽然这些外部指示灯有时不能提供具体的故障原因，但它能够为快速发现故障提供直接线索。例如，有一个路由器的风扇不能工作了，首先检查电源线和提供电源的电源模块是否正确连接，并检查电源指示灯。如果是绿色，说明风扇有电源连接，则风扇模块可能没有正确安装或已经损坏；如果是红色，说明至少有一个风扇发生故障，可先检查风扇是否被卡住。如果排除了风扇被卡住的情况后问题还存在，可更换风扇；如果指示灯不亮，则表明电源被关闭了。

其次，检查系统和启动日志。使用路由器提供的专用线缆，将计算机的串口连接到路由器的 CONSOLE 端口上。如果启动路由器，便可在超级终端上清楚地看到路由器的启动过程，在硬件自检过程中，如果发现错误，会在终端上显示错误提示信息，并记录在启动日志中。如果路由器能够找到 IOS 文件，并成功引导，则说明 IOS 没有问题。如果在 Flash 中没有找到 IOS 软件，则需要重新下载 IOS 到 Flash 中。从路由器的启动过程可以看出，IOS 引导完毕后，便将 Startup-Config 文件调入内存。如果不能成功地从 NVRAM 中找到启动配置文件，也需要重新下载。对于 IOS 和启动配置文件丢失的情况，可以在紧急情况下进入启动模式（这是常用于故障处理的模式），使用 TFTP 从计算机（此机的网卡必须使用交叉线连接到路由器的以太网络管理端口上）上启动和调入配置文件，临时救急。

再次，检查配置文件。配置文件有两种存在方式：启动配置文件和活动配置文件。前者是指保存在 NVRAM 上的启动文件。路由器启动后便调入此文件，进行路由器的具体配置，关机后不会丢失。活动配置文件是指在路由器的内存中正在运行的配置文件，关机或重启后会丢失。如果路由器刚刚启动，两者是一样的。如果管理员对路由器的配置进行了修改，并在内存中激活，这时两者是不一样的。为了方便管理员检查，有的系统还提供了专门的命令。很多初学者常常忘记把修改后的活动配置文件保存为启动配置文件，以致路由器下次启动时没有启用修改后的配置，仍然使用原来的配置文件，以至于怀疑路由器出现某种故障。

然后，检查配置内容。这是路由器故障检查的重中之重，因为路由器各种功能的实现都是由配置文件中的命令实现的。例如，接口地址的配置、路由协议的配置、ACL 的配置、SNMP 的配置、日志的配置、QoS 的配置、RMON 的配置、NAT 地址转换、端口的开关等。如果在配置中出现语法错误的语句，路由器会在初始化时显示错误提示，在 CLI（Command Line Interface，命令行接口）中配置时，也有错误提示，并会记录在系统日志中。配置过程中，因为有的语句必须放在某些语句的后面，所以要注意语句的顺序，同时还要注意注释语句的使用。

最后，检查硬件。在以上步骤中确定了某一方面的故障后，如果发现是硬件故障，则需要拆机更换硬件部件。除了经验外，故障排查过程中还可通过产品说明书、厂商网站获取支持。

6.3.3　网络故障排除命令

网络管理工具能够以图形化界面为用户快速提供动态的网络状态、统计信息和综合配置信

息。故障排除工具还包括欧姆表、数字万用表及电缆测试器、网络监测器、网络分析仪等。除此之外，网络命令也是常用的网络故障排查方法。

大多数交换机或路由器都提供大量的集成命令来帮助监视并对网络进行故障排除。例如，show 命令可以用于检测系统的安装情况与网络的正常运行状况，也可用于对故障区域的定位；ping 命令用于检测网络上不同设备之间的连通性；traceroute 命令可用于确定数据包在从一个设备到另一个设备直至目的地的过程中所经过的路径。

下面介绍的网络测试命令可以在 Windows 操作系统的 DOS 命令窗口中执行。

1．ping 命令

这个命令用来检测一帧数据从本地传送到目的主机所需的时间。它通过发送一些小的数据包并接收应答信息来确定两台计算机之间的网络连接情况。当网络出现故障时，ping 是第一个用到的工具，它可以有效地检测网络故障。

（1）语法格式

```
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count]
[[-j host-list]|[-k host-list]] [-w timeout] destination-list
```

（2）参数说明

- -t：不停地 ping 对方主机，直到按“Ctrl+C”组合键为止。
- -a：将地址解析为计算机名。如果想知道所 ping 的计算机名则使用该参数，计算机名一般在运行 ping 命令后的第一行显示。
- -n count：设置 ping 的次数，即设置用来测试而发送的测试数据包的个数，默认值为 4；测试数据包的个数由 count 的值决定。
- -l size：设置发送测试数据包的大小，默认值为 32 字节；测试数据包最大为 65 500 字节；超过这个数时，对方可能因接收的测试数据包太大而死机。
- -f：在测试数据包中发送“不要分段”标志。一般情况下，发送的测试数据包都会通过路由分段再发送给对方，添加此参数后，测试数据包就不会被网关分段处理。
- -i TTL：指定 TTL 值在对方系统中的停留时间，用来检查网络的运行情况。
- -v TOS：将“服务类型”字段设置为 TOS 指定的值。
- -r count：在“记录路由”字段中记录发送和返回测试数据包的路由。一般情况下，发送的测试数据包是通过一个个路由然后到达对方的，但是到底经过了哪些路由呢？通过此参数就可以设置探测经过的路由的个数，最大值为 9，即最多只能跟踪 9 个路由。
- -s count：设置 count 跃点数的时间戳。此参数与-r 差不多，只是这个参数不记录数据包返回所经过的路由。最多只记录 4 个。
- -j host-list：利用 host-list 设置计算机列表路由数据包，连续的计算机可以被中间网关分隔（路由稀疏源），IP 允许的最大数为 9。
- -k host-list：利用 host-list 设置计算机列表路由数据包，连续的计算机不能被中间网关分隔（路由密集源），IP 允许的最大数为 9。
- -w timeout：设置超时时间间隔，单位为 ms，默认值为 1000。
- destination-list：设置要测试的远程计算机名或 IP 地址。

命令参数非常多，但是常用的只有-a、-t、-n 和-w 四个。在使用过程中，可在 MS-DOS 提

示符下运行“ping”或“ping/？”命令来查看。

如果执行 ping 命令不成功，可以预测故障出现在以下几个方面：网线没有连通，网卡配置不正确，IP 地址不可用等。如果 ping 成功而网络仍无法使用，那么问题很可能出在网络系统的软件配置方面。ping 成功只能保证本地与目的主机存在一条连通的物理途径。

但是也存在例外的情况，即 ping“不通”但实际网络是连通的。这是因为某些操作系统的网络防火墙有可能将发来的 ping 命令数据包抛弃。在 ping 装有这样防火墙的主机时，将被告知“Request time out”，其实这并不表示网络不通。

2．iconfig 命令

与 ping 命令不同，利用 ipconfig 命令可以查看和修改网络中本地计算机与 TCP/IP 有关的配置信息，如 IP 地址、网关子网掩码等。

（1）语法格式

```
    ipconfig [/？|/all|/renew [adapter] | /release [adapter] | /flushdns |
/displaydns | /registerdns | /showclassid adapter | /setclassid adapter [classid] ]
```

（2）参数说明

- /？：显示本命令的帮助信息。
- /all：显示本地与 TCP/IP 相关的所有配置细节信息，包括主机名、节点类型、是否启用 IP 路由、网卡的物理地址、默认网关等。
- /renew：重建所有的或由 adapter 指定的适配器的 IP 地址。
- /release：释放所有的或由 adapter 指定的适配器的 IP 地址。
- /flushdns：清除 DNS 解析器高速缓存中的信息。
- /displaydns：显示 DNS 解析器高速缓存中的信息。
- /registerdns：刷新所有的 DHCP 租约，并重新注册 DNS 名称。
- /showclassid：显示由 adapter 指定的适配器的所有 DHCP 类型标识。
- /setclassid：修改 DHCP 类型标识。

常用的方法是不带任何参数或带参数/all。

3．tracert 命令

tracert 用于追踪“路径”，即可记录从本地至目的主机所经过的路径，以及到达时间。利用它，可以确切地知道究竟在本地到目的地之间的哪一环节发生了故障。

（1）语法格式

```
    tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name
```

（2）常用参数说明

- -d：不将地址解析为计算机名。
- -h maximum_hops：指定搜索目标地址的最大跳跃数。
- -j host-list：按照主机列表中的地址释放源路由。
- -w timeout：设置超时时间间隔，单位为 ms。
- target_name：目标计算机的名称。

4．netstat 命令

该命令用于显示协议统计信息和当前 TCP/IP 网络连接。

（1）语法格式

```
netstat [-a] [-b] [-e] [-n] [-o] [-s] [-p proto] [-r] [-s] [-v] [interval]
```

（2）常用参数说明

- -a：显示主机的所有连接和监听端口信息。
- -b：显示包含于创建连接或监听端口的可执行组件。在某些情况下已知可执行组件拥有多个独立组件，并且在这些情况下显示包含创建连接或监听端口的组件序列。这种情况下，可执行组件名在底部的[]中，顶部是其调用的组件，等等，直到 TCP/IP 部分。注意此选项可能需要很长时间，如果没有足够大的权限则可能失败。
- -e：显示以太网统计信息。此参数一般与-s 参数共同使用。
- -n：以数字表格格式显示地址和端口号。
- -o：显示与每个连接相关的所属进程 ID。
- -p proto：显示由 proto 指定的协议的具体使用信息。proto 可以是下列协议之一：TCP、UDP、TCPv6 或 UDPv6。
- -r：显示本机路由表的内容。
- -s：显示按协议统计的信息。默认显示 IP、IPv6、ICMPv6、TCP、ICMP、TCPv6、UDP 或 UDPv6 等协议的统计信息。
- -v：此参数与-b 参数共同使用时，将显示包含于为所有可执行组件创建连接或监听端口的组件。
- interval：重新显示所选的状态时每次显示之间的间隔，单位为 s。按“Ctrl+C”组合键将停止重新显示统计。如果省略，则 netstat 显示当前配置信息（只显示一次）。

6.3.4 典型故障排除示例

假设某信息网络的拓扑结构如图 6-5 所示。故障现象为 A 主机 ping 不通 B 主机。可综合采用前述分层与分段的故障排除思路，按如下步骤进行故障排查。

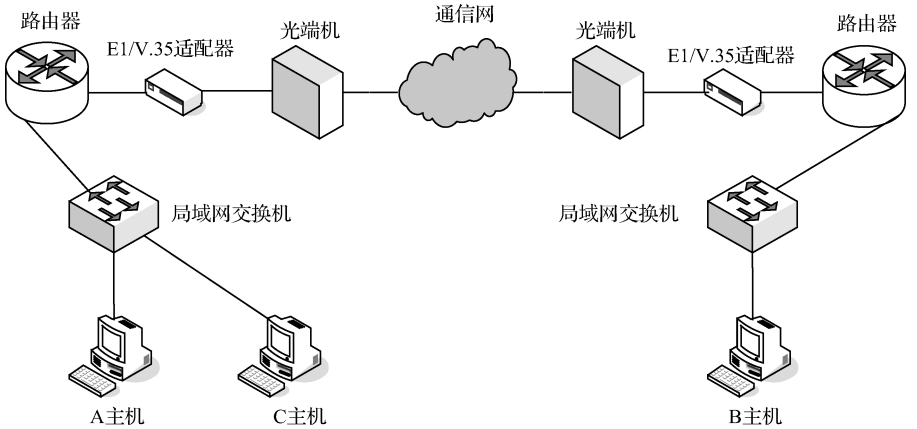


图 6-5　网络连接图

1．步骤一：局域网内部故障排查

在局域网内的另外一台 C 主机上，同时 ping A 主机与 B 主机，如图 6-6 所示。

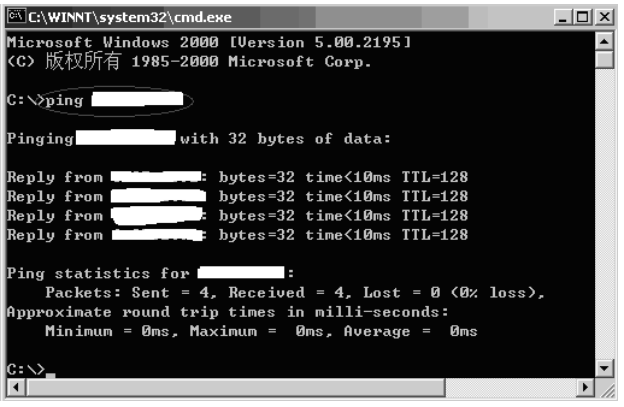


图 6-6　ping 命令的使用

现象 1：C 主机能够 ping 通 B 主机但 ping 不通 A 主机。

分析：A 主机的局域网接入存在问题。

解决方法如下。

（1）查看交换机的 LED 指示灯（主要是端口 LED 指示灯）。

（2）交换机正常工作情况下，有连接的端口的 LED 指示灯应为绿色，且会有闪烁。也可以在终端使用命令 show interface 进行判断，如图 6-7 所示。

图 6-7　网络交换机

（3）检查网卡设置是否正常。依次打开“控制面板/系统/设备管理/网络适配器”设置窗口，在该窗口中检查有无中断号及 I/O 地址冲突，如图 6-8 所示。

图 6-8　检查 I/O 冲突

（4）检查网线连线是否正常。网络连线故障通常包括网络线内部断裂，双绞线与 RJ45 水晶头之间接触不良。通常，可以使用测线仪来检测线路是否断裂，可以使用重新插拔的方法来检测双绞线与 RJ45 水晶头之间是否接触不良。

（5）检查网卡驱动程序安装是否正确。依次打开“控制面板/系统/设备管理器”，驱动程序安装不正确时，在设备名称前会出现黄色感叹号，如图 6-9 所示。

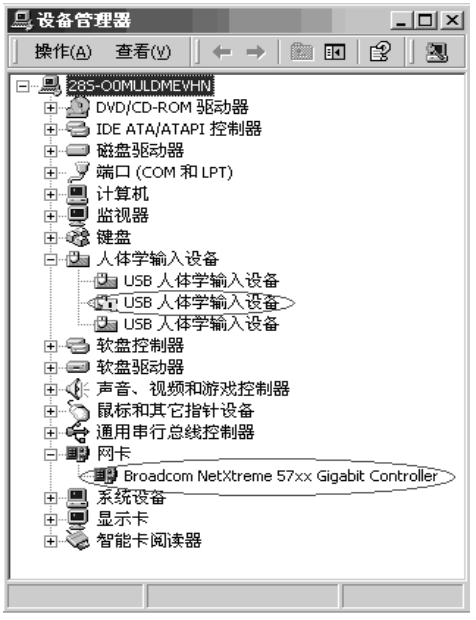


图 6-9　检查设备管理器

这时可以将网络适配器在系统配置中删除，然后重新启动计算机，系统就会检测到新硬件的存在，然后自动寻找驱动程序再进行安装。

（6）检查本机 IP 地址是否按规则进行设置，网关是否添加正确，如图 6-10 所示。

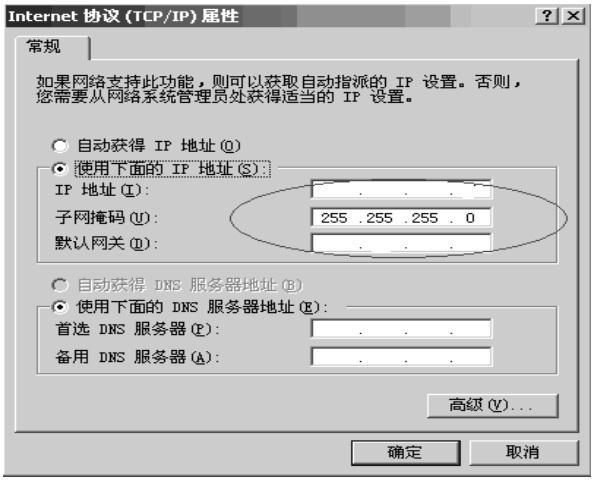


图 6-10　检查 IP 地址设置

现象 2：C 主机 ping 不通 B 主机但能 ping 通 A 主机。

分析：可以排除局域网内部的问题，问题出在局域网区域以外。

2．步骤二：网关故障排查

在 A 主机上 ping 本机网关的 IP 地址。

现象 1：ping 本机网关的 IP 地址超时。

分析：本地网络的路由器存在问题。

路由器故障主要由路由器模块接口故障和路由器软件 IOS 故障引起，通过观察模块接口处指示灯的亮、灭，在终端通过 show 命令可以判断模块接口是否工作正常，路由器软件 IOS 故障可以通过开机自动检测进行判断。如图 6-11 所示，正常工作时状态如表 6-1 所示。

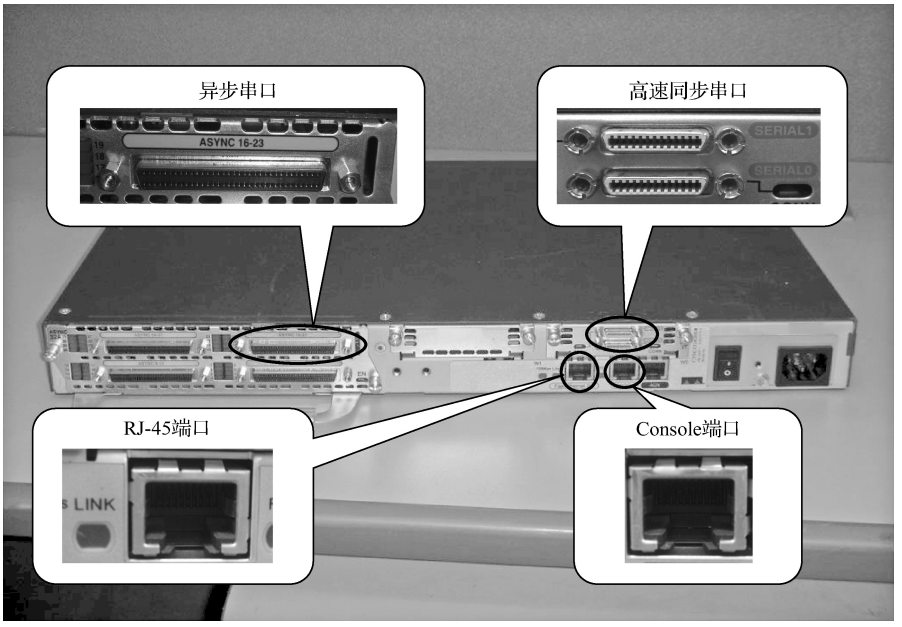


图 6-11　路由器的接口及其指示灯

表 6-1　路由器正常工作时指示灯状态

指示灯	POWER	ACTIVITY	100Mbps	LINK
正常状态	绿色	绿色闪烁	绿色	绿色

解决方法如下。

（1）检查连接交换机与路由器的双绞线、RJ45 水晶头之间是否接触不良。

（2）登录本地路由器，通过命令“show int fastethernet 0/0”查看快速以太网口状态，如图 6-12 所示。正常情况下，端口的物理层与链路协议层都应为“up”，同时查看端口的 IP 地址，IP 地址应与主机在同一网段。可通过“no shutdown”与“ip address”命令分别开启端口和配置 IP 地址。若是端口物理故障可以通过更换备用模块进行恢复；若是 IOS 软件故障，可以使用相关软件进行恢复。

现象 2：能 ping 通本机网关的 IP 地址。

分析：本地网络以外区域存在问题。

图 6-12　检查路由器端口

3．步骤三：本地路由器配置故障排查

登录本地路由器，查看路由协议配置是否正确，可以通过“sh ip protocols”命令检查，如图 6-13 所示，此时显示正常。

图 6-13　检查路由协议

4．步骤四：本地路由器对外路由故障排查

登录本地路由器，在路由器上追踪 B 主机的 IP 地址，如图 6-14 所示。

图 6-14　追踪路由器

现象 1：路由追踪从一开始就显示超时，如图 6-15 所示。

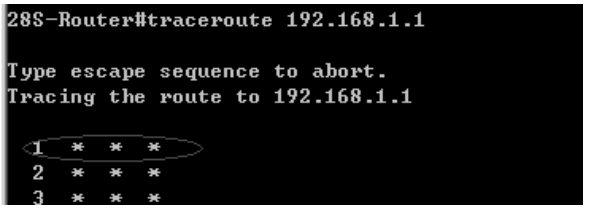


图 6-15　追踪超时

分析：数据包未能从源地址发送出去，接口转换器可能存在故障。

解决方法如下。

（1）通知光端机房保障人员查看对外连接光端机的工作状态，与远端协调解决。

（2）查看路由器 2M 接口所连接的 E1/V.35 接口转换器的状态指示灯，根据指示灯状态判断和解决故障。

（3）查看路由器 2M 接口所配置的链路层协议是否一致。通过“show int 接口”查看链路层封装的为何种协议，如图 6-16 所示。

现象 2：路由跟踪在中途显示超时。

分析：在源到目的地途中的某个节点由于某种原因路由数据包失败，造成超时。

解决方法：通知目的地光端与故障点所处的光端，彼此协调解决。

现象 3：路由追踪在到达目的地路由器后显示超时，无法到达 B 主机。

分析：数据包可以到达目的地路由器，说明源与目的地之间的广域网链路不存在问题。

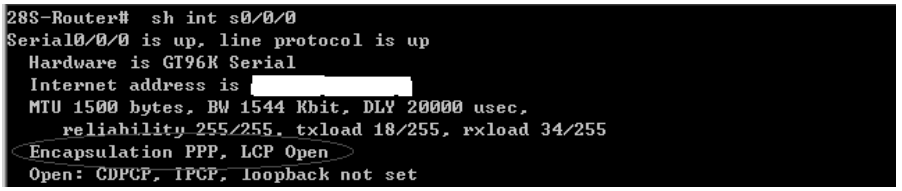


图 6-16　查看链路层协议

5．步骤五：目的网络故障排查

通过以上分段与分层排查，可以推测出故障存在于目的地路由器与交换机之间的网络或目的地局域网内。此时，可通知对方单位的技术人员按以上步骤一、步骤二、步骤三的方法进行排查，故障即可解决。

6．步骤六：目的地路由器故障排查

利用路由器的“show interfaces serial”命令输出的状态信息，判读其他接口故障、设备故障（见表 6-2）和线缆故障（见表 6-3）。

（1）现象 1：“Serial x is down，line protocol is down”。

可能的故障：路由器没有检测到载波信号，缆线故障或接口转换器硬件故障。

排除方法：

① 查看 LED 指示灯确定载波信号是否有效；

② 确保使用的是正确的缆线及接口；

③ 更换出现故障的部件；

④ 如果怀疑路由器硬件存在问题，可将串行线路连接到其他端口上。如果线路能正常工作，那么说明原先连接的接口存在故障。

（2）现象 2：“Serial x is down，line protocol is down”。

可能的故障：本地或远程路由器配置错误，远程路由器没有发送“keeplive”，本地或远程接口转换器出现故障，路由器硬件故障（本地或远程）。

排除方法：

① 在本地 E1/V.35 适配器或光端机上对本端打环，然后利用“show interfaces serial”命令确定线路协议是否工作正常。如果线路协议工作正常，那么问题可能在于远端路由器；

② 如果在本地打环的情况下，线路协议仍不正常，那么说明路由器硬件可能出现了故障。可以交换路由器的接口硬件；

③ 如果怀疑路由器硬件存在问题，可将串行线路连接到其他端口上。如果线路能正常工作，那么说明原先连接的接口存在故障。更换出现故障的部件即可。

（3）现象 3：“Serial x is up，line protocol is up（looped）”。

可能的故障：电路上存在环路。

排除方法：

① 利用“show running-config”命令查看路由器配置信息中是否存在包含“loopback”接口配置命令的条目；

② 如果路由器配置信息中存在包含“loopbacd”接口配置命令的条目，可以利用“no loopback”接口配置命令删除环路；

③ 如果路由器配置信息中没有包含“loopback”接口配置命令的条目，那么可以检查E1/V.35 适配器或光端机上是否被手工打环。

（4）现象 4：“Serial x is administratively down，line protocol is down”。

可能的故障：路由器配置信息中含有“shutdown”接口配置命令。

排除方法：

① 查看路由器配置信息中是否包含“shutdown”命令；

② 利用“no shutdown”命令消除“shutdown”命令的作用。

表 6-2 设备故障的排除

故障类型	可能的故障点	故障定位	故障分析	排故方法
设备故障	接口转换器	查看接口转换器的收发及 2M 告警指示灯	设备不能正常工作	使用“no shutdown”命令启用路由器端口或调换 2M 铜缆的收发
	路由器	利用“show version”命令查看显示的硬件接口是否与路由器上实际的硬件接口一致	出现故障的硬件接口不会在“show version”命令显示的列表中出现	模块化的接口更换模块，非模块化的接口更换路由器
	交换机	正常工作端口的指示灯状态应为绿色闪烁状，若一直为黄色闪烁状，则出现故障	交换机 nvram 中 VLAN 数据库的 VLAN 配置丢失	登录交换机重新配置 VLAN 即可

表 6-3 线缆故障的排除

故障类型	可能的故障点	故障定位	故障分析	排故方法
线缆故障	网线	交换机端口的指示灯不亮	网线头松动，金属片与双绞线没有接触上	换线或重新做水晶头
	路由器 V.35 线缆	利用“show interface”命令发现线路与协议都为“down”	物理层未连通	更换线缆
	2M 铜缆	2M 告警指示灯亮	收发反或线缆故障	更换线缆
	光缆	光端告警	收发反或线缆故障	更换光缆

习题

1．军事网络管理的内容有哪些？
2．军事网络管理有哪些方法？
3．简述 SNMP 网络管理技术的要点。
4．网络故障排除的一般方法是什么？
5．交换机有哪些常见故障？
6．路由器有哪些常见故障？
7．如何排查局域网内部的故障？

Chapter 7

第 7 章

军事网络安全

【主要内容】介绍军事网络安全的基本概念、常用的网络安全技术及网络病毒防护方法，包括军事网络的安全隐患、安全系统分类、安全设备功能，数据加密、防火墙、入侵检测、外联监控等网络安全技术的作用及其原理，以及网络病毒防治的方法与原则等。

7.1 军事网络安全概述

7.1.1 军事网络安全概念

军事网络安全是指军事信息系统中的硬件、软件及数据受到保护，不受偶然的或恶意的破坏、更改、泄露，从而系统能连续可靠正常地运行。军事网络安全包括物理安全和逻辑安全两个方面。其中，物理安全指系统设备及相关设施不受破坏和丢失，逻辑安全则指军事网络信息的安全。

1．安全隐患

从人为因素上看，军事网络存在无意和故意的安全隐患。无意事件包括操作失误、意外损失、编程缺陷、意外丢失、管理不善、无意破坏。人为故意的破坏主要指敌对势力蓄意攻击。

攻击是一种故意性威胁，是有意图、有目的的威胁。攻击可分为被动攻击和主动攻击两种。这两种攻击均可对军事网络造成极大的危害，导致数据泄露，甚至造成系统瘫痪，如图 7-1 所示。

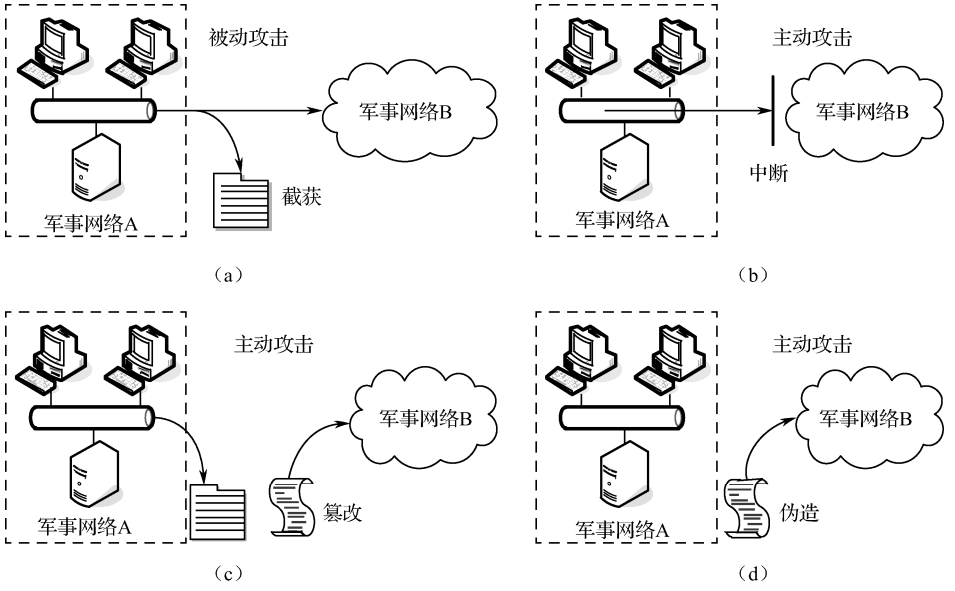


图 7-1　网络攻击的四种方法

（1）被动攻击

被动攻击是指在不影响系统正常工作的情况下，攻击者在系统上建立隐蔽通道截获、窃取和破译某一信息报文而不干扰信息流，以获得重要机密信息。被动攻击常常是主动攻击的前奏。被动攻击很难被发现，预防手段主要是加密传输的信息流，使得攻击者不能识别军事网络中所传输的信息内容。

（2）主动攻击

主动攻击有选择地更改、删除、延迟或伪造信息报文，破坏军事信息的可用性和完整性。主动攻击主要有三种方法。一是中断：攻击者故意中断他人在网络上的通信。二是篡改：是指网络中可能存在的某节点在非授权和不能监测方式下的数据修改，这些修改进入网中的帧并传送修改版本。三是伪造：是指网络中一个实体假扮成另一个实体收发信息。

数据加密、数据完整性校验、数字签名和访问控制等安全机制可以防范主动攻击，但杜绝主动攻击很困难，因此除了进行信息加密以外，对付主动攻击的另一措施是及时发现并恢复所造成的破坏，现在有很多实用的攻击检测工具。

2．网络安全内容

军事网络安全的内容主要有：

（1）网络实体安全

例如机房的物理条件、物理环境及设施的安全标准，计算机硬件系统、网络设备及网络传输线路的安装及配置等的安全。

（2）网络软件安全

例如保护军事网络不被非法侵入，系统软件与应用软件不被非法复制、篡改，不受病毒的侵害等。

（3）网络数据安全

例如保护军事网络中的数据不被非法存取，保护其完整一致等。

（4）网络安全管理

例如运行时突发事件的安全处理等，包括采取计算机安全技术、建立安全管理制度、开展安全审计、进行风险分析等内容。

总之，从信息应用的角度，军事网络的信息安全具有保密性、完整性、可用性和可控性四个特征。保密性，是指信息不泄露给非授权的用户、实体或过程；完整性，是指数据未经授权不能进行改变，即信息在存储或传输过程中保持不被修改、破坏、丢失或替代；可用性，是指可被授权实体按需访问和正常使用，即当需要时应能存取所需的信息。可控性，是指对信息的传播及内容具有控制能力。

3．网络安全控制

网络安全控制主要包括网络设备控制、路由交换控制和网络运行控制三个方面。

（1）网络设备控制

按要求设置网络设备操作各层次口令，防止非法操控网络设备；关闭远程用户登录，防范对设备的入侵；关闭不必要的服务，防止网络设备资源被不正当使用；限定用户服务资源，防止网络资源被恶意耗尽而导致设备失效。

（2）路由交换控制

进行链路层对等实体鉴别和接入验证，防止非法网络连接；进行必要的路由聚合，减少对外泄露网络结构信息；进行路由交换验证，防止非法窃取网络信息；控制接 El 流量，防止恶意侵占网络资源；进行路由总量控制，防止对网络实施冲击。

（3）网络运行控制

对网络工作状态阈值和涉及安全的操作进行预定义，当出现超过阈值的正常状态或发生可能影响网络安全性的操作时，自动向有关管理终端发出警告信息，为预防及处置提供有力保障，同时为审计提供必要数据。

4．安全服务

安全防护可使用一种或多种安全机制来提供保证。安全服务可分为以下六种。

① 保密性服务：保护信息不被泄露或暴露给未授权的实体（用户或系统）。

② 认证服务：提供某个实体的身份认证。

③ 数据完整性服务：保护数据以防止未授权的用户进行更改。

④ 非否认服务：防止参与某次通信交换的一方事后否认本次交换曾经发生过。

⑤ 访问控制服务：保护资源以免对其进行非法使用和操纵。

⑥ 可用性服务：保证信息与系统可被授权人利用。

7.1.2　军事网络安全系统

军事网络安全防护系统主要包含网络防火墙、入侵检测系统、非法外联监控、漏洞扫描器及网络病毒防护等系统。

1．网络防火墙

网络防火墙主要从逻辑上将受保护的内部网络与外部网络隔离，实现网络层的访问控制。

它安装在军事信息组网各个节点系统的出口处，可以在不改变原有网络应用系统结构的情况下，达到合理的安全防护要求，通过制定安全访问策略，可以检查、分析、过滤进出入内部网的 IP 包，尽可能对外部网络屏蔽被保护网络或节点的信息、结构，实现对内部网络的保护，减少网络受攻击的可能性。

2．入侵检测系统

入侵检测系统从网络的出口处收集信息并进行分析，检查网络中是否有违反安全策略的行为和遭到袭击的迹象。通过监听分析网上的数据流，实时跟踪、报警和阻断网络违规事件，对网络内部攻击、外部攻击和误操作进行保护，实现网络应用层及网络层上细粒度的入侵检测；对用户指定的网络资源情况、网络状态和网络操作行为可进行记录、查询、分析，为系统提供安全审计手段。

3．非法外联监控

实时监控系统内所有的服务器和席位计算机，随时发现并定位网内非法与其他网络建立连接的主机，根据预先制定的策略向安全管理员告警并向非法外联的主机发送警告消息。

4．漏洞扫描器

安全管理员在中央控制台使用漏洞扫描器模拟黑客的网络攻击手法，对系统中的所有或重点主机进行攻击性的安全漏洞和安全隐患扫描，提交风险评估报告，并提供相应的整改措施建议。安全管理员定期使用漏洞扫描器对网络中的主机进行安全性检查，可以最大限度地暴露网络中有安全漏洞的主机，准确报告安全漏洞的种类并提出修补措施。

5．网络病毒防护

网络防病毒主要是防止病毒对网络内服务器和终端的破坏，保证网络数据的安全性。该软件由服务器端杀毒模块、客户端杀毒模块及防病毒控制中心组成。服务器端杀毒模块安装在系统服务器上，客户端杀毒模块安装在用户终端上，防病毒控制中心安装在指定的服务器或用户终端上。通过制定合理的防病毒策略，可实时监测服务器和用户终端的文件及资源状况，发现病毒，及时报警与清除。防病毒软件的升级与分发由安全管理中心完成。

7.1.3 军事网络安全设备

军事网络安全防护设备对主机与其他网络设备提供集中的运行状态监控、事件获取和处理、策略管理、告警处置及值班管理，是进行网络监察的有效技术手段，是提供安全状态感知和决策支持的工具。

1．主要功能

（1）IP、MAC 绑定

将内部各主机的网卡 MAC 地址与 IP 地址绑定起来，主要用于防止受控的内部用户通过更换 IP 地址访问外网。

（2）流量控制

显示系统内部主机与外部广域网之间的实时网络流量情况，可根据 IP 地址、服务、用户等级等对流量进行控制，以防止线路资源的不正常消耗，有效地管理网络资源。

（3）网络访问控制

在系统局域网的网络出口设立网络报文检查点，根据网络数据报头信息（源 IP 地址、目的 IP 地址、源 TCP/UDP 端口、目的 TCP/UDP 端口、ICMP 报文类型域和代码域、TCP 标志位、时间等）设置过滤规则，控制局域网内所有主机与外部广域网的双向网络通信。

（4）网络入侵检测

从网络出口处收集信息并进行分析，检查网络中是否有违反安全策略的行为和遭到袭击的迹象。通过监听分析网上的数据流，实时跟踪、报警和阻断网络违规事件，对网络内部攻击、外部攻击和误操作进行保护，实现网络应用层及网络层上细粒度的入侵检测。

（5）安全告警处置

记录边界访问的行为与入侵事件的简要分析，提供事件告警的处置操作，如进行上传管理中心、事件小结等操作。

（6）安全值班管理

记录安全事件处置过程、结果，提供值班日志的历史查询和报表输出；提供班次信息管理功能，向上级安全管理中心上报安全管理报告。

（7）补丁管理

集中管理上级下发的补丁，并提供向系统上传、下载补丁的功能，包括病毒库升级、漏洞修补、OS 补丁升级等操作，从而提高本地信息网络的安全防护能力。

2．部署位置

安全防护设备以透明方式接入网络系统，对网络拓扑没有影响。其典型的框架应用方式如图 7-2 所示。安全防护设备位于路由器和交换机之间，为内部网络安全提供有力的保障。安全管理终端实现系统管理、参数配置、策略管理和系统审计等安全管理功能。

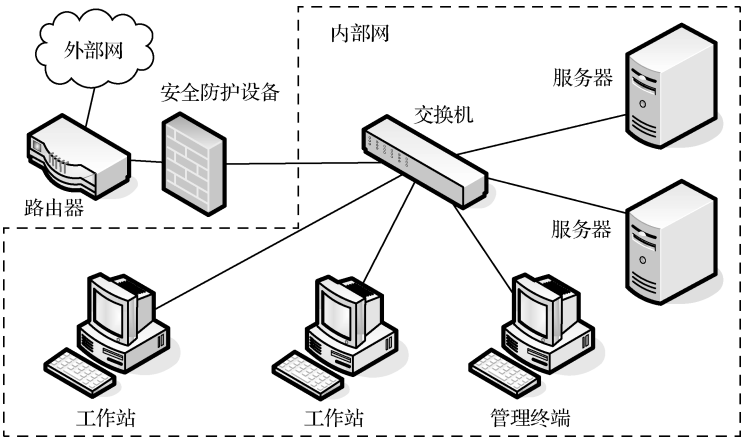


图 7-2　网络安全设备部署示意图

7.2 网络安全技术

为了保护军事网络安全，必须在军事信息系统中使用各种网络安全防护技术。军事信息系统的网络安全涉及病毒防御、漏洞扫描、补丁分发、入侵检测等技术，军事信息系统的计算机主机安全涉及数据加密、密钥管理、信息隐藏、信息认证、访问控制、病毒防治、安全审计技术、漏洞扫描和防电磁泄漏等技术。归纳起来，数据加密技术、防火墙技术、入侵检测技术、非法外联监控技术等是保证设备与系统安全的基础。

7.2.1 数据加密技术

所谓加密算法就是作用于密钥和明文（或密文）的一个数学函数。一般的数据加密模型如图 7-3 所示。在发送端，明文 X 用加密算法 E 和加密密钥 K 得到密文 Y。在传送过程中可能出现密文截取者。接收端接收到密文后，利用解密算法 D 和解密密钥 K，解出明文为 X。截取者即攻击者或入侵者。加密密钥和解密密钥具有相关性，这里假定两者是相同的。

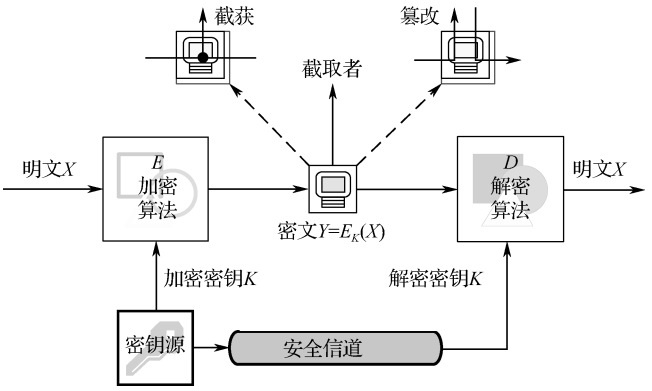


图 7-3 一般的数据加密模型

如果截取者截获了密文，但在密文中没有足够的信息来唯一地确定出对应的明文，则这一密码体制称为无条件安全的，或称为理论上是不可破的。在无限制条件下，目前几乎所有实用的密码体制在理论上均是可破的。如果一个密码体制中的密码不能被可以使用的计算资源破译，则这一密码体制称为在计算上是安全的。

与数据加密伴随而来的是密钥的安全和管理问题。对数据信息的加密和解密来说，密钥是安全的关键。密钥是加密和解密过程中使用的一串数字，通常由一个密钥源提供。在同一种加密算法下，密钥的位数越长，安全性越好。当密钥需要向远地传送时，一定要使用另一个安全信道传输。

目前使用最为广泛的主要有私人密钥法、公共密钥法和数字签名技术三种方法。

1．私人密钥法

私人密钥法也称对称加密法或常规密钥加密法，是一种使用相同的密钥对信息进行加密和

解密的技术。其中最有影响的是 1977 年美国国家标准局颁布的数据加密标准算法，如图 7-4 所示。

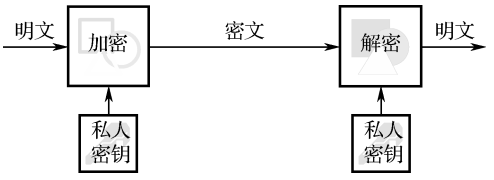


图 7-4　私人密钥法

私人密钥法加密技术的特点是算法简单、速度快；被加密的数据块长度可以很长；发送者和接收者共有一个双方同意的密钥，并且不被其他任何人所知晓，但这种方法很麻烦并且容易出错。因为每个人都会持有多个密钥，以便用于不同的目的。

2．公共密钥法

20 世纪 70 年代中期，出现了公共密钥加密技术，又称非对称加密法。通过公共密钥加密，每个人都可有一对密钥，一个是公共的，另一个是私人的。每人的公共密钥将对外发布，而私人密钥被秘密保管。其典型代表是 1978 年美国麻省理工学院 R. L. Rivest 等人提出的 RSA 公开密码算法。

当 A 想要发送一个报文给 B 时，A 就使用 B 的公共密钥将其报文加密后发送出去。当 B 得到该密文后，B 用自己的私人密钥进行解密。这样，发送者和接收者在进行秘密通信时，就不必非得共用一个密钥了，如图 7-5 所示。

图 7-5（a）说明加密明文使用的是收件人的公共密钥，然后使用收件人的私人密钥解密密文，这将保证只有指定的收件人（假设他是收件人密钥的唯一拥有者）才能解密邮件。

图 7-5（b）说明了另一种加密方法，在这里明文使用发件人的私人密钥进行加密，并使用发件人的公共密钥解密。这种方法为数字签名提供了基础。

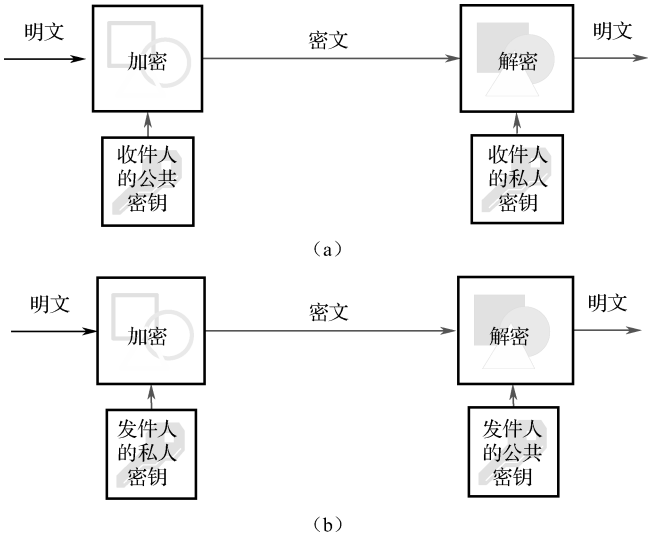


图 7-5　公用密钥法

公共密钥加密技术的特点是速度慢，被加密的数据块长度不宜太大；公钥在加密方和解密

方之间传递和分发可不必通过安全通道进行。因为加密密钥不等于解密密钥，并且在计算上不能由加密密钥推出解密密钥，所以将加密密钥公开也不会危害解密密钥的安全。

3．数字签名技术

书信或文件根据亲笔签名或印章来证明其真实性。但在军事网络中传送的文电又如何盖章呢？这就要使用数字签名。数字签名必须实现以下三点功能。

（1）接收者能够核实发送者对报文的签名。接收者能够确信该报文的确是发送者发送的，其他人无法伪造对报文的签名，也称为报文鉴别。

（2）接收者确信所收到的数据和发送者发送的完全一样而没有被篡改过，也称为报文的完整性。

（3）发送者事后不能抵赖对报文的签名，也称为不可否认。

现在已有多种数字签名方法，但采用公钥算法比采用对称密钥算法更容易实现。下面介绍这种数字签名方法。

为了进行签名，A 用其私钥 SKA 对报文 *X* 进行 *D* 运算。*D* 运算本来叫作解密算法。还没有加密怎么就进行解密呢？这并没有关系。因为 *D* 运算只是得到了某种不可读的密文。在图 7-6 中写上的是“*D* 运算”而不写上“解密运算”就是为了避免产生这种误解。A 把经过 *D* 运算得到的密文传送给 B。B 为了核实签名，用 A 的公钥 PKA 进行 *E* 运算，还原出明文 *X*。请注意，任何人用 A 的公钥 PKA 进行 *E* 运算后都可以得出 A 发送的明文。可见图 7-6 中的 *D* 运算和 *E* 运算都不是为了解密和加密，而是为了进行签名和核实签名。

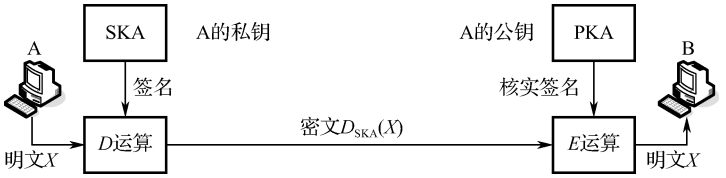


图 7-6　数字签名的实现

因为除 A 外没有别人持有 A 的私钥 SKA，所以除 A 外没有别人能产生密文 D_{SKA}（*X*）。这样，B 就相信报文 *X* 是 A 签名发送的，这就是报文鉴别的功能。同理，其他人如果篡改过密文，但因无法得到 A 的私钥 SKA 来对 *X* 进行加密，B 对篡改过的报文进行解密后将会得出不可读的明文，就知道收到的报文被篡改过。这样就保证了报文完整性的功能。若 A 要抵赖曾发送报文给 B，B 可把 *X* 及 D_{SKA}（*X*）出示给进行公证的第三者。第三者很容易用 PKA 去证实 A 确实发送了 *X* 给 B，这就是不可否认的功能。这里的关键都是没有其他人能够持有 A 的私钥 SKA。

7.2.2　防火墙技术

为避免网络信息被非法浏览、复制、修改、删除等非授权行为的发生，对访问者的信息资源使用权限需要进行控制，该功能主要通过防火墙来实施。防火墙是内部网络与外部网络间的一道屏障，内部网络被认为是安全和可信赖的，而外部网络被认为是不安全和不可信赖的。防火墙的作用是防止不希望的、未经授权的通信进出被保护的内部网络，实现网络层的访问控制。

它通过制定安全访问策略，检查、分析、过滤进出入内部网的 IP 包，控制内部网络与外部网络间的数据流量，屏蔽外部网络的非法入侵，保护内部网络信息、结构。防火墙的位置与作用如图 7-7 所示。

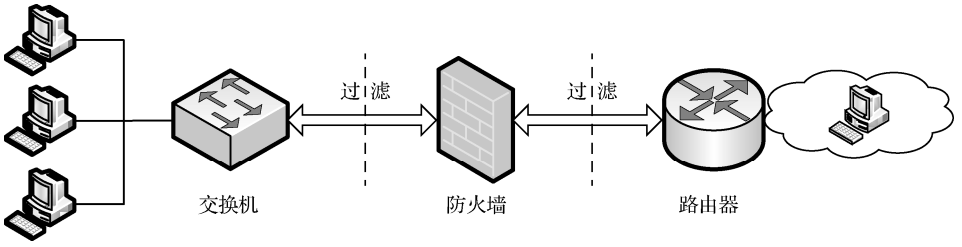


图 7-7　防火墙的位置与作用

1．防火墙的基本概念

计算机网络防火墙是用一个或一组网络设备（计算机系统或路由器等）在两个网络之间执行控制策略的系统，以保护一个网络不受另一个网络攻击的安全技术。防火墙的组成可以表示为：防火墙=过滤器+安全策略（+网关）。它可以监测、限制、更改进出网络的数据流，尽可能地对外部屏蔽被保护网络内部的信息、结构和运行状况，以此来实现网络的安全防护。防火墙的设计和应用基于这样一种假设：防火墙保护的内部网络是可信赖的网络，而外部网络则是不可信赖的网络。设置防火墙的目的是保护内部网络资源不被外部非授权用户使用，防止内部受到外部非法用户的攻击。

防火墙的主要功能包括：检查所有从外部网络进入内部网络的数据包；检查所有从内部网络流出到外部网络的数据包；执行安全策略，限制所有不符合安全策略要求的分组通过；具有防攻击能力，保证自身的安全性。

2．防火墙的类型

根据所采用的基本技术不同，防火墙可分为基本型防火墙和混合型防火墙两大类。基本型防火墙有数据包过滤防火墙和应用级网关。混合型防火墙将以上两种基本型防火墙结合使用，主要包括主机屏蔽防火墙和子网屏蔽防火墙。

（1）数据包过滤防火墙

数据包过滤防火墙也称为数据包过滤路由器，是一种基于路由器技术的、最简单的防火墙。数据包过滤防火墙技术在网络层对数据包进行分析、选择，选择的依据是系统内设置的数据包过滤规则（即访问控制表）。通过检查数据流中每个数据包的源地址、目的地址、所用的端口号、协议状态或它们的组合等因素来确定是否允许该数据包通过。

数据包过滤防火墙的优点是：结构简单，便于使用和管理，易于实现对用户透明地访问，且费用较低。它通常安装在路由器上（数据包过滤路由器由此而得名），因此在原有网络上增加这样的防火墙几乎不需要任何额外的费用。

（2）应用级网关

应用级网关也称为双宿主网关或应用型防火墙，其物理位置与数据包过滤路由器一样，但它的逻辑位置在应用层上。应用级网关技术在网络的应用层上实现协议过滤和转发功能。应用级网关在应用层过滤进出内部网络特定服务的用户请求与响应。如果应用级网关认为用户身份与服务请求、响应是合法的，就会将服务请求转发到相应的服务器或主机；如果应用级网关认

为服务请求与响应是非法的，就将拒绝用户的服务请求，丢弃相应的包，并向网络管理员报警。图 7-8 所示为应用级网关原理示意图。

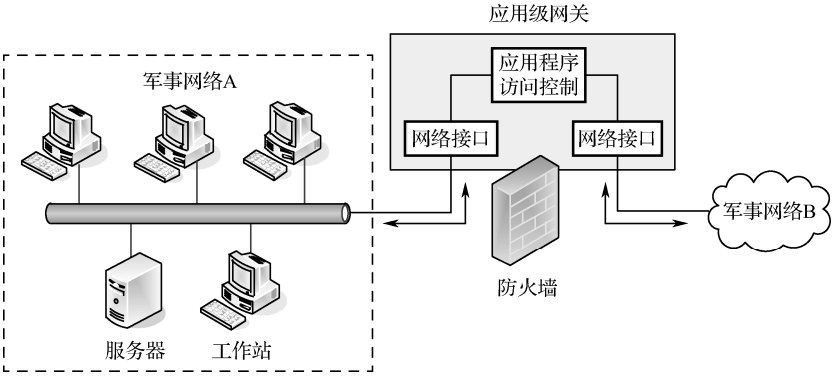


图 7-8　应用级网关原理示意图

应用代理是应用级网关的另一种形式，但是它们的工作方式不同。应用级网关以存储转发方式检查和确定网络服务请求的用户身份是否合法，决定是转发还是丢弃该服务请求的数据包。因此从某种意义上说，应用级网关在应用层“转发”合法的应用请求。应用代理与应用级网关的不同之处在于：应用代理完全接管了用户与服务器的访问，隔离了用户主机与被访问服务器之间的数据包交换通道。在实际应用中，应用代理的功能是由代理服务器实现的，原理如图 7-9 所示。

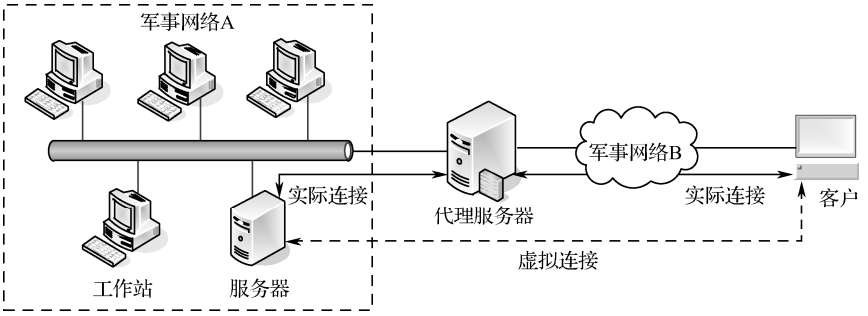


图 7-9　应用代理的基本原理示意图

应用代理的工作原理：当外部网络主机用户希望访问内部网络的某服务器时，应用代理截获用户的服务请求。如果检查后确定为合法用户，允许访问该服务器，那么应用代理将代替该用户与内部网络的某服务器建立连接，完成用户所需要的操作，然后将结果回送给请求服务的用户。对于外部网络的用户来说，它好像是“直接”访问了该服务器，而实际访问服务器的是应用代理。应用代理应该是双向的，它既可以作为外部网络主机用户访问内部网络服务器的代理，也可以作为内部网络主机用户访问外部网络服务器的代理。由于外部网络与内部服务器之间没有直接数据通道，外部的恶意侵害也就很难伤害到内部网络。

应用级网关与应用代理的优点是可以针对某一特定的网络服务，并能在应用层协议的基础上分析与转发服务请求与响应。同时它们一般都具有日志记录功能。日志中记录了网络上所发生的事件，管理员可以根据日志监控可疑的行为并进行相应的处理。由于应用级网关与应用代理只使用一台计算机，因此易于建立和维护。如果要支持不同的网络服务，则需要配备不同的应用服务代理软件。

（3）主机屏蔽防火墙

主机屏蔽防火墙由一个只需单个网络端口的应用级网关和一个数据包过滤路由器组成，是目前较流行的一种防火墙。它物理地连接在网络总线上，它的逻辑功能仍工作在应用层上，所有业务通过它进行代理服务。内部网络不能直接通过路由器和外部网络相联系，数据包要通过包过滤路由器和堡垒主机两道防线。如图 7-10 所示，主机屏蔽防火墙设置了两层安全保护，因此相对比较安全。

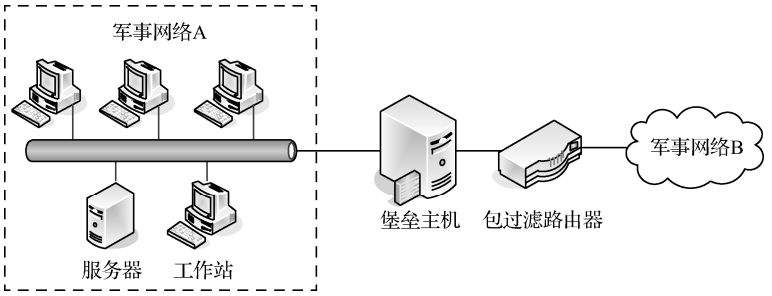


图 7-10　主机屏蔽防火墙的基本原理示意图

堡垒主机是指运行防火墙软件的主机，其作用是转发应用、提供服务、监督通信。主机屏蔽防火墙的第一个安全设施是包过滤路由器，对来自外部网络的数据包而言，首先要经过数据包过滤路由器的过滤，过滤后的数据包被转发到堡垒主机上，然后由堡垒主机上的应用服务代理对这些数据包进行分析，将合法的信息转发到内部网络的主机上。外出的数据包首先经过堡垒主机上的应用服务代理检查，然后被转发到数据包过滤路由器，最后由数据包过滤路由器转发到外部网络上。

（4）子网屏蔽防火墙

子网屏蔽防火墙的保护作用比主机屏蔽防火墙更进了一步，它在被保护的内部网络与外部网络之间加入了一个由两个包过滤路由器和一台堡垒机组成的子网。被保护的内部网络与外部网络不能直接通信，而是通过各自的路由器和堡垒主机通信，两台路由器也不能直接交换信息，如图 7-11 所示。

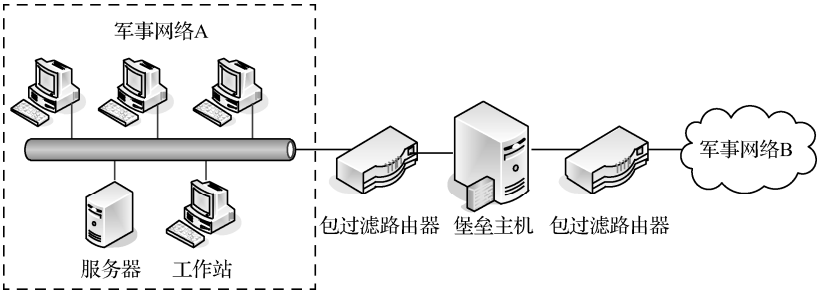


图 7-11　子网屏蔽防火墙的基本原理示意图

子网屏蔽防火墙是最为安全的一种防火墙体系结构，它具有主机屏蔽防火墙的所有优点，并且更加优越。

7.2.3　入侵检测技术

入侵检测技术从网络的若干个关键点收集信息，分析网络中是否有违反安全策略的行为和

遭到袭击的迹象，是否有来自网络外部和内部的入侵信号及网络系统是否存在漏洞。扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。入侵检测技术包括入侵检测和漏洞检测。

1．入侵检测

入侵检测在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。其功能有：监视分析用户和系统的行为；查找非法用户和合法用户的越权操作；审订系统配置和安全漏洞并提示管理员修补漏洞；评估敏感系统和数据的完整性、识别攻击行为；对异常行为进行统计，自动收集与系统相关的补丁，进行审计跟踪，识别违反安全法规的行为；使用诱骗服务器记录黑客行为等。这些检测功能使系统管理员可以有效地监视、审计、评估自己的系统。

检测到一个入侵攻击后，向监测中心报告（经常是实时的），然后就可以采取措施阻止该攻击。入侵实时检测系统基于对用户历史行为建立的模型，以及根据早期的证据建立的模型。审计系统实时地检测用户对系统的使用情况，根据系统保持的用户行为的概率统计模型进行监测，当发现有可疑的用户行为发生时，保持跟踪并监测，记录该用户的行为。

网络入侵检测系统大多采用分布式结构。采用分布式的基于主机的和基于网络的入侵检测系统相结合的综合方案，既可以克服基于主机的入侵检测系统和基于网络的入侵检测系统的不足，又可以充分发挥它们各自的优势，从而实现对被保护目标的最佳防护，其检测机制见图 7-12。

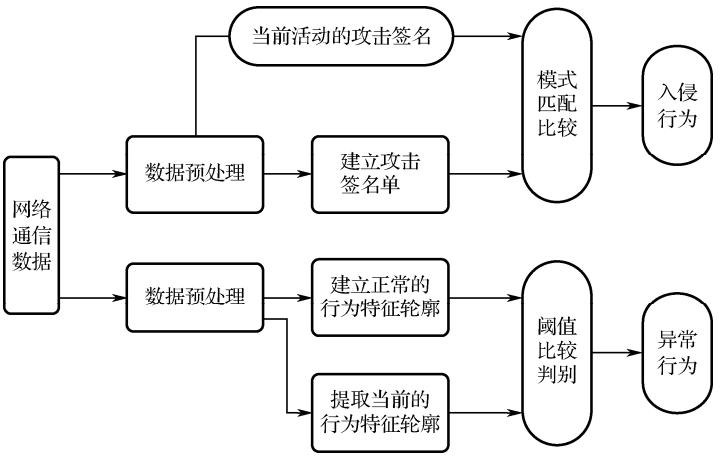


图 7-12　分布式入侵检测系统检测机制

2．漏洞检测

漏洞检测是指基于漏洞数据库，通过扫描等手段对军事信息系统进行检查，发现网络系统远端或本地计算机系统中可被黑客利用的漏洞。漏洞扫描系统结构图如图 7-13 所示。

漏洞扫描实际上是对系统安全性能的评估，指出易受攻击的漏洞，为补丁分发提供警示信息。漏洞扫描与补丁分发工具将这信息记录并发送到网络化安全防护服务中心的数据库中。

进行漏洞扫描时，在管理控制台的用户界面可以设置扫描方案，针对不同的网络状况形成不同的检测策略；中心管理部分制订扫描任务，维护安全策略，提供限制访问，调度扫描检测模块；漏洞检测部件通过分布式的扫描代理对目标系统的各项漏洞进行检查，并提供脆弱性等级及相应风险防范建议。

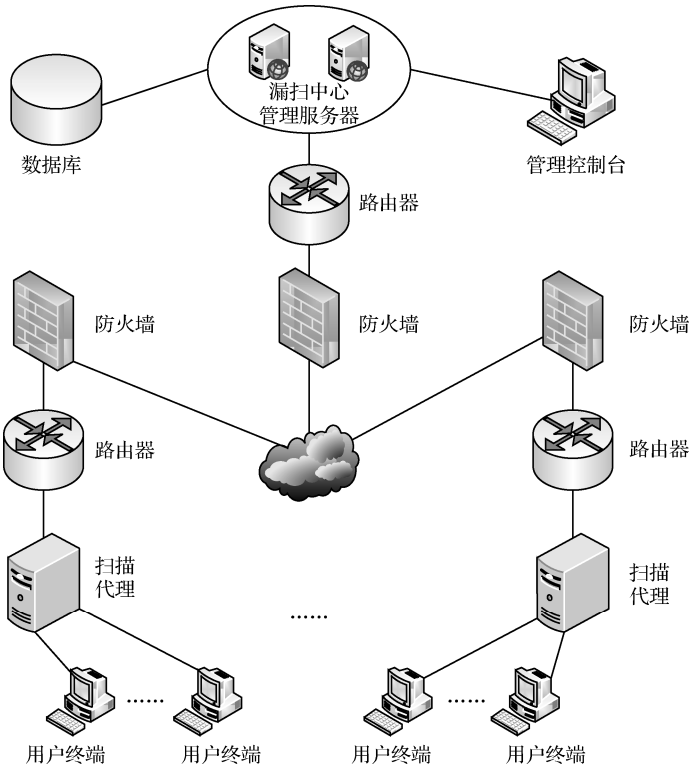


图 7-13　漏洞扫描系统结构图

7.2.4　非法外联监控技术

在军事网络的内部网和外部网之间安装防火墙和入侵检测系统，基本可以保护内部网不受入侵。但是，内部网的主机通过隐蔽通道连接外部网特别是因特网，成为一个极其危险又非常难以察觉的安全隐患。内部主机通过调制解调器、ADSL 拨号设备、双网卡、无线网卡等网络设备非法接入外部网络，它轻易地从内部网络撕开一条通向外部的秘密通道，绕过了整个网络边界的安全防护措施（如防火墙、网络监控工具）的监控，对内部网络的安全构成极大威胁。

非法外联可以定义为：内部网终端计算机内外网线交叉错接、内部网终端计算机使用拨号、无线网卡、双网卡等方式接入外网、便携式笔记本电脑接入内部网络使用，事后又接入外部网使用。这些人为有意或无意的疏忽，在内部网与外部网间开出新的连接通道，外部的黑客攻击或病毒能够绕过原本连接在内部网和外部网之间的防护屏障，顺利侵入非法外联的计算机，盗窃内部网的敏感信息和机密数据，造成泄密事件，甚至利用该机作为跳板，攻击、传染内部网的重要服务器，导致整个内部网工作瘫痪。

内部网终端计算机潜在许多与外界联系的通道，要保证内外网的物理隔离效果，重点是切断内部网终端计算机与外部网联系的途径。对在线（正在内网使用）的客户端，根据管理策略要求，灵活地开启或关闭每个客户端的各种外联途径，同时对离开了内部网的移动设备，关闭其一切外联方法，强制性地使其成为“信息孤岛”，真正维护内部网的封闭性。

非法外联监控系统的安全模型：在安装客户端软件的计算机（以下简称客户端）之间构成

一个相互信任的安全域，可以相互通信，客户端与非客户端的网络连接称为外联。当管理策略允许外联时，客户端可以主动与非客户端通信，其外联行为将记录在案，非客户端不允许与客户端主动通信（这种主动通信定义为非法入侵）；当管理策略不允许外联时，客户端与非客户端不允许通信，非客户端主动与客户端联系视为入侵，如图 7-14 所示。

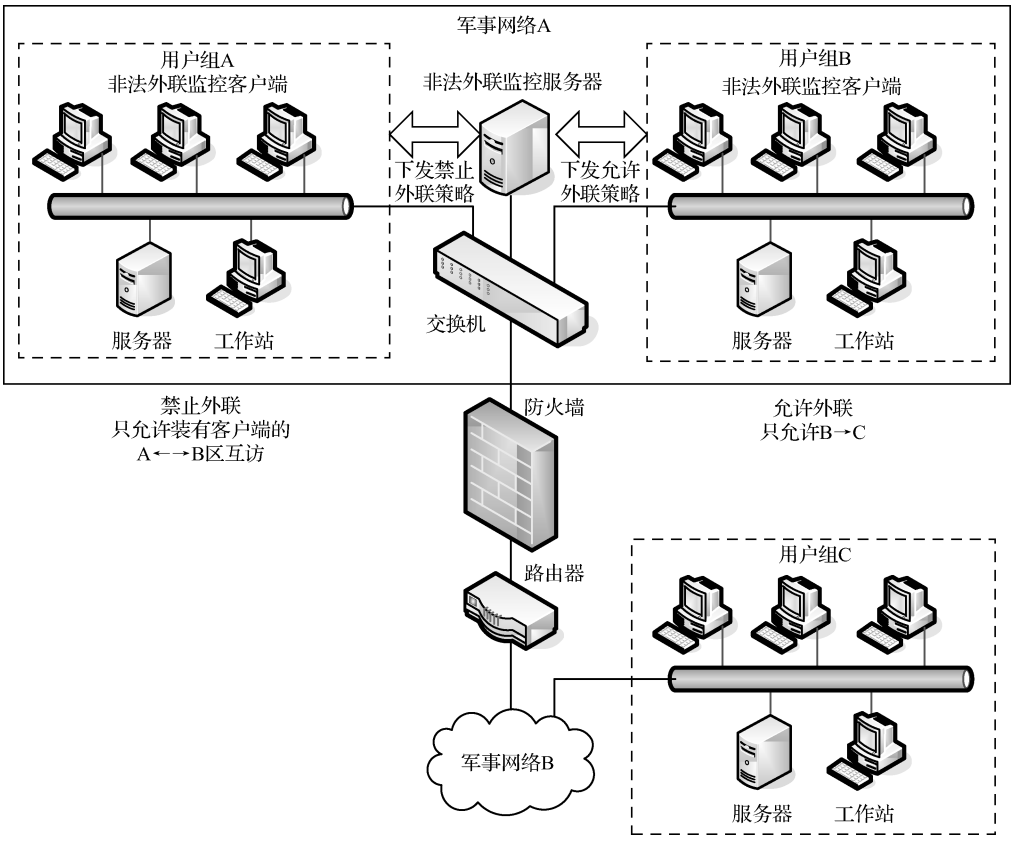


图 7-14　非法外联监控系统原理图

非法外联监控系统管理策略分为在线策略和非在线策略，这两种策略都包含了网络连接策略、I/O 设备使用策略。客户端在线（能连接到服务端）时，实施在线安全管理策略；客户端不在线时，实施非在线安全管理策略。根据实际管理需要，这两组策略可以相同也可以不相同，根据需要灵活设置。一般来说，在线策略设置为不允许外联，以维护内部网的封闭性；可以使用 I/O 设备，以方便办公。客户端离开了局域网后，非在线策略生效，一般情况下，非在线策略不允许外联，不允许使用 I/O 设备，以保证离开内网的客户端不与外界发生任何联系，达到维护内网封闭性的目的。

7.3 网络病毒防护

“计算机病毒”与医学上的“病毒”不同，它不是天然存在的，是某些人利用计算机软件或硬件所固有的脆弱性，编制出的具有特殊功能的可执行的小程序。

在网络环境下，病毒可以按指数增长模式进行传染。病毒侵入军事网络，可以导致军事网

络效率急剧下降、系统资源遭到严重破坏，短时间内造成网络系统瘫痪。因此网络环境下病毒防治是军事网络应用的必要环节。

1．网络病毒的特点

（1）传染方式多

病毒入侵网络的主要途径是通过席位计算机传播到服务器硬盘中，再由服务器传播到其他席位计算机。

（2）传染速度快

由于病毒在网络中传染速度非常快，使其扩散范围很大，不但能迅速传染局域网内所有席位计算机，还能通过远程席位计算机将病毒在一瞬间传播到千里之外。

（3）清除难度大

在单机上，再顽固的病毒也可通过删除带毒文件、格式化硬盘等措施将病毒清除，而网络中只要有一台席位计算机未能杀毒干净就可使整个网络重新全部被病毒感染，甚至刚刚完成杀毒工作的一台席位计算机就有可能被网上另一台席位计算机的带毒程序所传染，因此，仅对席位计算机进行病毒杀除不能彻底解决网络病毒问题。

（4）破坏性强

网络上的病毒将直接影响网络的工作，轻则降低速度，影响工作效率，重则造成网络系统瘫痪，破坏服务器系统资源，使多年工作毁于一旦。

2．网络病毒的防治方法

网络环境下的病毒防治应采用统一的防病毒策略，实时扫描、监控、预防、查杀病毒，消除病毒传播途径，防止病毒感染及破坏。基于服务器的病毒防治方法主要有以下几种。

（1）实时在线扫描

网络防毒技术必须保持全天 24 小时监控网络中是否有带毒文件进入服务器。为了保证病毒监测实时性，通常采用多线程的设计方法，让检测程序作为一个随时可以激活的功能模块。且在网络运行环境中，不影响其他线程的运行。当网络用户将带毒文件有意或无意复制到服务器中时，网络防毒系统必须立即通知网络管理员，同时自动记入病毒档案。

（2）服务器扫描

对服务器中的所有文件集中检查是否带毒。若有带毒文件，则提供几种处理方法给网络管理员，允许用户清除病毒或删除带毒文件，或者更改带毒文件名成为不可执行文件名并隔离到一个特定的病毒文件目录中。

允许网络管理员定期检查服务器中是否带毒，如可每月、每星期、每天集中扫描网络服务器，这样网络用户拥有极大的操作选择余地。

（3）席位计算机扫描

基于服务器的防毒软件并不能保护本地席位计算机的硬盘，一个有效方法是在服务器上安装防毒软件的同时，在上网的席位计算机内存中调入一个常驻扫毒程序，实时监测席位计算机中运行的程序。

3．个人病毒的防治原则

为了防治计算机病毒，个人对席位计算机的日常使用应注意以下事项。

（1）不使用盗版或来历不明的软件。

（2）绝不把用户数据写到系统盘上。

（3）安装真正有效的防毒软件，并经常进行升级。

（4）新购买的计算机在使用之前首先要进行病毒检查，以免机器带毒。

（5）准备一张干净的系统引导盘，此后一旦系统受“病毒”侵犯，就可以使用该盘引导系统，然后进行检查、杀毒等操作。

（6）对外来程序要使用尽可能多的杀毒软件进行检查（包括从硬盘、移动硬盘、局域网、Internet、E-mail 中获得的程序），未经检查的可执行文件不能复制入硬盘，更不能使用。

（7）经常对重要数据进行备份，防患于未然。

（8）在安装了重要应用软件后对系统盘进行镜像备份，以便随时恢复操作系统到某种使用状态。

（9）随时注意计算机的各种异常现象（如速度变慢、出现奇怪的文件、文件尺寸发生变化、内存减少等），一旦发现，应立即用杀毒软件仔细检查。

碰到病毒之后的解决办法如下。

（1）在解毒之前，要先备份重要的数据文件。

（2）启动反病毒软件，并对整个硬盘进行扫描。

（3）发现病毒后，一般应利用杀毒软件清除文件中的病毒，如果可执行文件中的病毒不能被清除，一般应将其删除，然后重新安装相应的应用程序，或者恢复系统到某种镜像状态。

（4）某些病毒在 Windows 状态下无法完全清除，此时应采用事先准备的干净的系统引导盘引导系统，然后在 DOS 下运行相关杀毒软件进行清除。

习题

1．军事网络有哪些安全隐患？

2．军事网络可以采用哪些安全防护系统？

3．简述数据加密技术的原理。

4．防火墙有哪些类别？各有什么特点？

5．简述入侵检测技术的原理。

6．简述外联监控技术的原理。

7．简述网络病毒防治的主要方法。

参 考 文 献

[1] 谢希仁. 计算机网络（第 6 版）. 北京：电子工业出版社，2014.
[2] 刘勇. 计算机网络基础. 北京：清华大学出版社，2016.
[3] 张保通. 网络互联技术. 北京：中国水利水电出版，2009.
[4] 王相林. 计算机网络. 北京：机械工业出版社，2008.
[5] 肖川. 局域网技术与组网工程. 北京：北京理工大学出版社，2011.
[6] 李光明. 计算机网络技术教程. 北京：人民邮电出版社，2009.
[7] 黄子俊. 情报组网系统原理与维修. 空军预警学院，2012.
[8] 石志国. 计算机网络安全教程（修订版）. 北京：清华大学出版社，2010.
[9] 高素清. 数据通信基础. 北京：科学出版社，2001.
[10] 童志鹏. 综合电子信息系统. 北京：国防工业出版社，2008.
[11] 李恒勋. 战场信息系统. 北京：国防工业出版社，2003.
[12] 郑连清. 战场网络战. 北京：军事科学出版社，2002.
[13] 曾宪钊. 国家基础设施和军事网络. 北京：电子工业出版社，2016.
[14] 张乃平. 计算机网络技术. 广州：华南理工大学出版社. 2015.
[15] 苏锦海. 军事信息系统. 北京：电子工业出版社，2010.
[16] 韩林. 军事电子信息系统安全. 北京：军事科学出版社，2002.
[17] 胡昌平. 信息服务与用户. 武汉：武汉大学出版社，2001.
[18] 谢希仁. 计算机网络（第五版）. 北京：电子工业出版社，2008.
[19] 白涛. 网络工程实施技术与方案大全. 北京：电子工业出版社，2008.
[20] 高传善. 数据通信与计算机网络. 北京：高等教育出版社，2007.
[21] 龚向阳. 宽带通信网原理. 北京：北京邮电学院出版社，2006.
[22] 李桂华. 信息服务设计与管理. 北京：清华大学出版社，2009.
[23] 郭振安. 网络信息资源重组理论与实践. 北京：兵器工业出版社，2004.
[24] 寇雅楠. 网络技术及其军事应用. 北京：国防工业出版社，2014.
[25] 汤永利. 信息安全管理. 北京：电子工业出版社，2017.

反侵权盗版声明